

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
BUTTE DIVISION**

**IN RE: SNOWFLAKE, INC., DATA
SECURITY BREACH LITIGATION**

2:24-MD-03126-BMM

**LIVE NATION
ENTERTAINMENT INC. AND
TICKETMASTER L.L.C.'S
MEMORANDUM IN
SUPPORT OF ITS MOTION
TO DISMISS OR,
ALTERNATIVELY, MOTION
TO STRIKE THE CONSUMER
PLAINTIFFS' THIRD
AMENDED
REPRESENTATIVE CLASS
ACTION COMPLAINT**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	FACTUAL BACKGROUND.....	4
A.	Ticketmaster’s Privacy Policy and Terms of Use	5
B.	Ticketmaster’s Security Measures and Snowflake	9
C.	The Data Potentially Impacted	12
D.	Plaintiffs and Their Lawsuits	13
III.	PROCEDURAL BACKGROUND	16
IV.	LEGAL STANDARD	17
A.	Rule 12(b)(1)	17
B.	Rule 12(b)(6)	17
C.	Rule 12(f)	18
D.	Applicable Choice of Law.....	20
V.	ARGUMENT.....	22
A.	Plaintiffs Cannot Establish Article III Standing.....	22
1.	<i>Plaintiffs’ Claimed Injuries Do Not Confer Standing</i>	25
2.	<i>Plaintiffs Fail to Allege Traceability</i>	34
B.	California Plaintiffs’ Claims Under the California Consumer Privacy Act Fail.....	37
1.	<i>The California Plaintiffs’ CCPA Claim</i>	38
2.	<i>California Plaintiffs Cannot Assert a Cognizable CCPA Claim</i>	39

i.	<i>Incomplete Payment Card Data Without CVV Codes Are Not “Personal Information” for Purposes of CCPA’s Private Right of Action</i>	40
ii.	<i>The California Plaintiffs Fail to Plead that California Passport Numbers Were Included in the Data Incident</i>	41
3.	<i>California Plaintiffs Lack Standing to Assert a CCPA Claim</i>	43
C.	<i>Plaintiffs’ Breach of Contract Claims Fail</i>	44
1.	<i>Plaintiffs Cannot Identify Any Breached Contractual Provisions</i>	44
2.	<i>Plaintiffs’ Damages Are Not Recoverable by Contract</i>	49
3.	<i>Plaintiffs’ Breach of Implied Contract Claims Also Fail</i>	51
i.	<i>There Is No Implied Duty to Protect Plaintiff’s Data</i>	52
D.	<i>Plaintiffs’ Negligence Claims Fail</i>	53
1.	<i>The Negligence Claims Are Barred by the Economic Loss Doctrine</i>	54
2.	<i>Plaintiffs Cannot Prove Causation</i>	56
3.	<i>Plaintiffs Cannot Prove Damages</i>	57
E.	<i>Montana Plaintiffs’ MCPA Claim Fails</i>	58
F.	<i>California Plaintiffs’ Unfair Competition Law Claim Fails</i>	61
G.	<i>Plaintiffs Fail to State A Claim Under GBL § 349</i>	65
VI.	<i>CONCLUSION</i>	65
	<i>CERTIFICATE OF COMPLIANCE</i>	68

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Ables v. Brooks Bros. Grp.</i> , No. CV 17-4309-DMG (EX), 2018 WL 8806667 (C.D. Cal. June 7, 2018)	30
<i>Adams v. Cole Haan, LLC</i> , No. SACV 20-913, 2020 WL 5648605 (C.D. Cal. Sept. 3, 2020)	62
<i>Aguilar v. RP MRP Wash. Harbour, LLC</i> , 98 A.3d 979 (D.C. 2014)	54
<i>Albrecht v. Comm. on Emp. Benefits of the Fed. Reserve Emp. Benefits Sys.</i> , 357 F.3d 62 (D.C. Cir. 2004).....	51
<i>Anderson v. ReconTrust Co., N.A.</i> , 407 P.3d 692 (Mont. 2017).....	59-60
<i>In re Apple Processor Litig.</i> , No. 22-16164, 2023 WL 5950622 (9th Cir. Sept. 13, 2023).....	62-63
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	18, 42, 52
<i>Barros v. Gov’t Emps. Ins. Co., Inc.</i> , 79 F. Supp. 3d 32 (D.D.C. 2015).....	44
<i>Bass v. Facebook, Inc.</i> , 394 F. Supp. 3d 1024 (N.D. Cal. 2019).....	35, 50, 56
<i>Baton v. Ledger SAS</i> , 740 F. Supp. 3d 847 (N.D. Cal. 2024).....	48
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	17-18, 41
<i>Berkley v. Dowds</i> , 152 Cal. App. 4th 518 (2007)	53

<i>Beverage Distribs., Inc. v. Olympia Brewing Co.</i> , 440 F.2d 21 (9th Cir. 1971)	46
<i>Black v. IEC Grp., Inc.</i> , No. 1:23-CV-00384-AKB, 2024 WL 3623361 (D. Idaho July 30, 2024)	26
<i>Bock v. Washington</i> , 33 F.4th 1139 (9th Cir. 2022)	26
<i>Brown v. 1301 K St. Ltd. P’ship</i> , 31 A.3d 902 (D.C. 2011)	50
<i>Buckles v. BH Flowtest, Inc.</i> , 476 P.3d 422 (Mont. 2020).....	20-21
<i>Capiau v. Ascendum Mach., Inc.</i> , No. 3:24-CV-00142-MOC-SCR, 2024 WL 3747191 (W.D.N.C. Aug. 9, 2024)	27
<i>Caronia v. Philip Morris USA, Inc.</i> , 5 N.E.3d 11 (N.Y. 2013).....	24
<i>Castillo v. Prime Hydration LLC</i> , 748 F. Supp. 3d 757 (N.D. Cal. 2024).....	64
<i>Cintron v. Title Fin. Corp.</i> , No. CV 17-108-M-DLC, 2018 WL 692936 (D. Mont. Feb. 1, 2018)	18-19
<i>City of Los Angeles v. Lyons</i> , 461 U.S. 95 (1983).....	23
<i>Clapper v. Amnesty Int’l USA</i> , 568 U.S. 398 (2013).....	23-24
<i>Cooper v. Bonobos, Inc.</i> , No. 21-CV-854-JMF, 2022 WL 170622 (S.D.N.Y. Jan. 19, 2022)	31
<i>Corp. Air v. Pratt & Whitney Canada Corp.</i> , No. CV 08-33-BLG-RFC, 2009 WL 10701737 (D. Mont. Aug. 21, 2009)	21

<i>Courthouse News Serv. v. Planet</i> , 750 F.3d 776 (9th Cir. 2014)	17
<i>Cumis Ins. Soc’y, Inc. v. BJ’s Wholesale Club, Inc.</i> , 918 N.E.2d 36 (Mass. 2009)	54
<i>D’Ambrosio v. Engel</i> , 741 N.Y.S.2d 42 (App. Div. 2002)	54
<i>Diep v. Apple, Inc.</i> , No. 22-16514, 2024 WL 1299995 (9th Cir. Mar. 27, 2024)	64
<i>Doe I v. GitHub, Inc.</i> , 672 F. Supp. 3d 837 (N.D. Cal. 2023)	43
<i>Ebomwonyi v. Sea Shipping Line</i> , 473 F. Supp. 3d 338 (S.D.N.Y. 2020)	44
<i>Est. of Petersen v. Koelsch Senior Cmtys., LLC</i> , No. CV 22-11-BLG-SPW-TJC, 2025 WL 953709 (D. Mont. Feb. 21, 2025)	60
<i>Est. of Rogel v. City of Bozeman</i> , No. 24-cv-034-BU-BMM, 2025 WL 1249223 (D. Mont. Apr. 30, 2025)	17-18
<i>In re Facebook, Inc. Internet Tracking Litig.</i> , 956 F.3d 589 (9th Cir. 2020)	44
<i>Flynn v. FCA US LLC</i> , No. 15-CV-0855-MJR-DGW, 2016 WL 5341749 (S.D. Ill. Sept. 23, 2016)	19, 34
<i>Friends of the Earth, Inc. v. Laidlaw Env’t Servs., Inc.</i> , 528 U.S. 167 (2000)	23
<i>Gardiner v. Walmart Inc.</i> , No. 20-CV-04618-JSW, 2021 WL 2520103 (N.D. Cal. Mar. 5, 2021)	40
<i>Gardiner v. Walmart, Inc.</i> , No. 20-CV-04618-JSW, 2021 WL 4992539 (N.D. Cal. July 28, 2021)	34

<i>Gibson v. Jaguar Land Rover N. Am., LLC</i> , No. CV 20-00769-CJC, 2020 WL 5492990 (C.D. Cal. Sept. 9, 2020)	62
<i>Greenstein v. Noblr Reciprocal Exch.</i> , No. 22-17023, 2024 WL 3886977 (9th Cir. Aug. 21, 2024).....	35
<i>Griffey v. Magellan Health Inc.</i> , 562 F. Supp. 3d 34 (D. Ariz. 2021)	52
<i>Guthridge v. Johnson & Johnson Corp.</i> , No. 22-CV-145-BLG-SPW-TJC, 2023 WL 6626175 (D. Mont. Sept. 22, 2023)	61
<i>Hammerling v. Google LLC</i> , 615 F. Supp. 3d 1069 (N.D. Cal. 2022).....	51
<i>Hemphill v. Horne, LLP</i> , No. 3:24-CV-178-KHJ-ASH, 2025 WL 837007 (S.D. Miss. Mar. 10, 2025)	27
<i>Hochendoner v. Genzyme Corp.</i> , 823 F.3d 724 (1st Cir. 2016).....	34
<i>Holmes v. SIPC</i> , 503 U.S. 258 (1992).....	56
<i>Hunter v. Benefis Health Sys., Inc.</i> , No. 21-CV-92-GF-BMM, 2024 WL 664709 (D. Mont. Feb. 16, 2024)	4
<i>I.C. v. Zynga, Inc.</i> , 600 F. Supp. 3d 1034 (N.D. Cal. 2022).....	26, 30-31
<i>In re Illuminate Educ. Data Sec. Incident Litig.</i> , No. SACV 22-1164 JVS (ADSx), 2023 WL 3158954 (C.D. Cal. Apr. 19, 2023)	26
<i>Indem. Ins. Co. of N. Am. v. Expeditors Int’l of Wash., Inc.</i> , 533 F. Supp. 3d 158 (S.D.N.Y. 2021)	50

<i>Jackson v. Loews Hotels, Inc.</i> ED18-CV-827-DMG-JCX, 2019 WL 6721637 (C.D. Cal. July 24, 2019)	32-34
<i>Johnson v. Yuma Reg’l Med. Ctr.</i> , No. CV-22-01061-PHX-SMB, 2024 WL 4803881 (D. Ariz. Nov. 15, 2024)	24
<i>Kearns v. Ford Motor Co.</i> , 567 F.3d 1120 (9th Cir. 2009)	64
<i>Kemper Ins. Cos., Inc. v. Fed. Exp. Corp.</i> , 115 F. Supp. 2d 116 (D. Mass. 2000)	50
<i>Knievel v. ESPN</i> , 393 F.3d 1068 (9th Cir. 2005)	5
<i>Koenigsberg v. Bd. of Trs. of Columbia Univ.</i> , No. 23 CIV. 1044 (PGG), 2024 WL 1256270 (S.D.N.Y. Mar. 22, 2024)	65
<i>Kostecky v. Peas in a Pod LLC</i> , 518 P.3d 840 (Mont. 2022)	58
<i>Kraut v. City of New York</i> , 925 N.Y.S.2d 624 (App. Div. 2011)	53
<i>Krefting v. Kaye-Smith Enters. Inc.</i> , No. 2:23-CV-220, 2023 WL 4846850 (W.D. Wash. July 28, 2023)	51-52
<i>Krystofiak v. BellRing Brands, Inc.</i> , 737 F. Supp. 3d 782 (N.D. Cal. 2024)	64
<i>Kuhns v. Scottrade, Inc.</i> , 868 F.3d 711 (8th Cir. 2017)	51-53
<i>Leavitt v. Brockton Hosp., Inc.</i> , 907 N.E.2d 213 (Mass. 2009)	53
<i>Lewis v. Casey</i> , 518 U.S. 343 (1996)	43

<i>Liau v. Weee! Inc.</i> , No. 23-CV-1177-PAE, 2024 WL 729259 (S.D.N.Y. Feb. 22, 2024)	30
<i>Lindstrom v. Polaris Inc.</i> , No. CV 23-137-BLG-SPW-TJC, 2024 WL 4237732 (D. Mont. Aug. 9, 2024)	44
<i>Lowy v. Daniel Def., LLC</i> , No. 1:23-CV-1338, 2024 WL 3521508 (E.D. Va. July 24, 2024)	56
<i>Lujan v. Defs. of Wildlife</i> , 504 U.S. 555 (1992).....	43
<i>In re Macbook Keyboard Litig.</i> , No. 5:18-cv-02813-EJD, 2020 WL 6047253 (N.D. Cal. Oct. 13, 2020)	62
<i>Maryland Cas. Co. v. Asbestos Claims Ct.</i> , 460 P.3d 882 (Mont. 2020).....	57
<i>McCombs v. Delta Grp. Elecs., Inc.</i> , 676 F. Supp. 3d 1064 (D.N.M. June 9, 2023)	26
<i>McNulty v. Bewley Corp.</i> , 596 P.2d 474 (Mont. 1979).....	51
<i>Miron v. Herbalife Int’l, Inc.</i> , 11 F. App’x 927 (9th Cir. 2001)	49
<i>Montana Wildlife Fed’n v. Bernhardt</i> , No. 4:18-CV-69-BMM, 2021 WL 4865257 (D. Mont. June 21, 2021)	23
<i>Morales v. Conifer Revenue Cycle Sols., LLC</i> , No. 2:23-CV-01987-AB-AGR, 2025 WL 1096396 (C.D. Cal. Mar. 31, 2025)	25
<i>Papageorge v. Zucker</i> , 169 A.3d 861 (D.C. 2017)	53
<i>Pearl v. Coinbase Global, Inc.</i> , No. 22-CV-03561, 2024 WL 3416505 (N.D. Cal. July 15, 2024)	55

<i>Pegasus Trucking, LLC v. Asset Redeployment Grp., Inc.</i> , No. 19-CV-10339, 2021 WL 1234879 (C.D. Cal. Feb. 16, 2021)	55
<i>Pruchnicki v. Envision Healthcare Corp.</i> , 845 F. App’x 613 (9th Cir. 2021)	24-25, 27
<i>Quinalty v. FocusIT LLC</i> , No. CV-23-00207-PHX-JJT, 2024 WL 342454 (D. Ariz. Jan. 30, 2024)	57
<i>Ramos v. Wells Fargo Bank, N.A.</i> , No. 23-CV-0757, 2023 WL 5310540 (S.D. Cal. Aug. 17, 2023).....	55
<i>Randolph v. ING Life Ins. & Annuity Co.</i> , 973 A.2d 702 (D.C. 2009)	24
<i>Razuki v. Caliber Home Loans, Inc.</i> , No. 17-CV-1718-LAB, 2018 WL 6018361 (S.D. Cal. Nov. 15, 2018)	18
<i>Reidy v. UMass Mem’l Med. Ctr., Inc.</i> , No. 2085-CV-01101, 2021 WL 6777622 (Mass. Super. Ct. June 17, 2021)	24
<i>In re Residential Capital, LLC</i> , 529 B.R. 806 (Bankr. S.D.N.Y. 2015).....	55
<i>Rohrer v. Knduson</i> , 203 P.3d 759 (Mont. 2009).....	58-59
<i>SAA-A, Inc. v. Morgan Stanley Dean Witter & Co.</i> , 721 N.Y.S.2d 640 (App. Div. 2001).....	51
<i>In re Samsung Data Sec. Breach Litig.</i> , 761 F. Supp. 3d 781 (D.N.J. Jan. 3, 2025)	36
<i>Schertz v. Ford Motor Co.</i> , No. CV 20-03221-TJH, 2020 WL 5919731 (C.D. Cal. July 27, 2020)	62
<i>Sheen v. Wells Fargo Bank, N.A.</i> , 505 P.3d 625 (Cal. 2022).....	54

<i>Sifuentes v. X Corp.</i> , No. 24-CV-00590-SK, 2024 WL 4953431 (N.D. Cal. Dec. 2, 2024)	42
<i>Sikorski v. Johnson</i> , 143 P.3d 161 (Mont. 2006).....	53
<i>Smahaj v. Retrieval-Masters Creditors Bureau, Inc.</i> , 131 N.Y.S.3d 817 (N.Y. Sup. Ct. 2020).....	46
<i>Sonner v. Premier Nutrition Corp.</i> , 971 F.3d 834 (9th Cir. 2020)	62-63, 65
<i>In re Sony Gaming Networks & Customer Data Sec. Breach Litig.</i> , 903 F. Supp. 2d 942 (S.D. Cal. 2012).....	48
<i>Southland Sod Farms v. Stover Seed Co.</i> , 108 F.3d 1134 (9th Cir. 1997)	58-59
<i>Spokeo, Inc. v. Robins</i> , 578 U.S. 330 (2016).....	43
<i>Squeri v. Mount Ida Coll.</i> , 954 F.3d 56 (1st Cir. 2020).....	44
<i>Storm v. Paytime, Inc.</i> , 90 F. Supp. 3d 359 (M.D. Pa. 2015).....	22
<i>Sullivan v. O’Connor</i> , 961 N.E.2d 143 (Mass. App. Ct. 2012)	51
<i>In re SuperValu, Inc.</i> , 870 F.3d 763 (8th Cir. 2017)	28
<i>Talbot v. Ainuu</i> , No. CV-23-66-BU-BMM, 2024 WL 896370 (D. Mont. Mar. 1, 2024)	20
<i>Tarter v. Throne L. Off., P.C.</i> , No. 17-CV-123-BLG-SPW, 2019 WL 462985 (D. Mont. Feb. 6, 2019)	24

<i>Terpin v. A.T. & T Mobility LLC</i> , 118 F.4th 1102 (9th Cir. 2024)	54
<i>Thompson v. Neb. Mobile Homes Corp.</i> , 647 P.2d 334 (Mont. 1982)	53
<i>TransUnion LLC v. Ramirez</i> , 594 U.S. 413 (2021)	23-24, 26
<i>Travis v. Assured Imaging LLC</i> , No. CV-20-00390-TUC-JCH, 2021 WL 1862446 (D. Ariz. May 10, 2021)	29-30
<i>Tsao v. Captiva MVP Rest. Partners, LLC</i> , 986 F.3d 1332 (11th Cir. 2021)	28-29
<i>Ebeid ex rel. U.S. v. Lungwitz</i> , 616 F.3d 993 (9th Cir. 2010)	63
<i>United States v. Hossain</i> , No. 22-16085, 2023 WL 5319262 (9th Cir. Aug. 18, 2023)	19
<i>United States v. Rhodes</i> , No. CV 21-110-M-DLC-KLD, 2023 WL 129859 (D. Mont. Jan. 9, 2023)	19
<i>Wallace v. Health Quest Sys., Inc.</i> , No. 20-CV-545, 2021 WL 1109727 (S.D.N.Y. Mar. 23, 2021)	46
<i>Weaver v. Aetna Life Ins. Co.</i> , No. 308-CV-00037-LRH-VPC, 2008 WL 4833035 (D. Nev. Nov. 4, 2008)	49, 57
<i>Webb v. Rejoice Delivers LLC</i> , No. 22-CV-07221-BLF, 2025 WL 974996 (N.D. Cal. Apr. 1, 2025)	62-63
<i>Whalen v. Michaels Stores, Inc.</i> , 689 F. App'x 89 (2d Cir. 2017)	29
<i>White v. Lee</i> , 227 F.3d 1214 (9th Cir. 2000)	17

<i>Winsor v. Sequoia Benefits & Ins. Servs., LLC</i> , 62 F.4th 517 (9th Cir. 2023)	35
<i>In re Zappos.com, Inc.</i> , 888 F.3d 1020 (9th Cir. 2018)	29
<i>In re Zappos.com, Inc.</i> , No. 3:12-CV-00325-RCJ, 2013 WL 4830497 (D. Nev. Sept. 9, 2013)	46

Statutes

28 U.S.C. § 1407	16
Cal. Bus. & Prof. Code § 17200	61
Cal. Civ. Code § 1798.81.5(d)(1)(A).....	38
Cal. Civ. Code § 1798.81.5(d)(1)(A)(iii).....	41
Cal. Civ. Code § 1798.82(h)	40
Cal. Civ. Code § 1798.150(a)(1).....	38, 42
California Consumer Privacy Act.....	<i>passim</i>
Mont. Code Ann. § 28-2-702	49
Mont. Code Ann. § 28-3-102	20-21
Montana Unfair Trade Practices & Consumer Protection Act	58, 60-61
New York’s General Business Law § 349.....	65
Unfair Competition Law	61-63, 65

Rules & Regulations

FED. R. CIV. P. 8	61
FED. R. CIV. P. 9	65
FED. R. CIV. P. 9(B)	61, 63-64
FED. R. CIV. P. 11	22
FED. R. CIV. P. 12(B)(1).....	1, 17, 38, 65
FED. R. CIV. P. 12(B)(6).....	1, 17, 38, 65
FED. R. CIV. P. 12(F).....	1, 18, 65

Other Authorities

Live Nation Entertainment, Inc., Annual Report (Form 10-K) (Feb. 22, 2024), https://investors.livenationentertainment.com/sec-filings/annual-reports/content/0001335258-24-000017/0001335258-24-000017.pdf ;	10
Mandiant, <i>UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion, Google Cloud</i> (June 10, 2024), https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion	10
Restatement (Second) of Conflict of Laws.....	20
Restatement (Second) of Torts.....	31, 57
Snowflake, <i>Snowflake Security Hub</i> , https://www.snowflake.com/en/why-snowflake/snowflake-security-hub/ (last visited June 16, 2025).....	9, 45
Ticketmaster, <i>Our Commitments</i> , https://web.archive.org/web/20230517182539/https://privacy.ticketmaster.com/our-commitments (archived May 17, 2023)	47
Ticketmaster, <i>Privacy Policy</i> , https://web.archive.org/web/20240226041015/https://privacy.ticketmaster.com/privacy-policy#contact-us (archived Feb. 26, 2024)	6

Ticketmaster, *Terms of Use*,
[https://help.ticketmaster.com/hc/en-us/articles/10468830739345-](https://help.ticketmaster.com/hc/en-us/articles/10468830739345-Terms-of-Use)
Terms-of-Use (last updated July 2, 2021)*passim*

Ticketmaster, *Ticketmaster Data Security Incident*,
[https://help.ticketmaster.com/hc/en-us/articles/26110487861137-](https://help.ticketmaster.com/hc/en-us/articles/26110487861137-Ticketmaster-Data-Security-Incident)
Ticketmaster-Data-Security-Incident (last visited June 16, 2025) 11-12, 14

Pursuant to Rules 12(b)(1), 12(b)(6), and 12(f) of the Federal Rules of Civil Procedure, Defendants Live Nation Entertainment, Inc. (“Live Nation”) and Ticketmaster L.L.C. (collectively, “Ticketmaster”) move to dismiss, or, alternatively, move to strike Consumer Plaintiffs’ Third Amended Representative Class Action Complaint (“Complaint”) (ECF No. 427). For the reasons stated below, the Court should dismiss the Complaint in its entirety, or, in the alternative, strike portions of Plaintiffs’ Complaint.

I. INTRODUCTION

As one of the world’s largest entertainment companies, Ticketmaster works hard to protect customer data. From the moment it is collected, Ticketmaster implements a number of safeguards to protect its customers’ information, including implementing numerous industry-standard security measures. Indeed, none of Ticketmaster’s systems or customer accounts were impacted by this Data Incident¹ perpetrated by cyber criminals, and Plaintiffs make no such allegation. Instead, the breach affected a third-party data storage and analytics platform, Snowflake, Inc. (“Snowflake”), used by Ticketmaster and many other companies.

When Ticketmaster uses third-party providers like Snowflake, Ticketmaster ensures that the third party has its own cybersecurity program designed to keep the information secure. Unfortunately, Ticketmaster’s Snowflake account, like

¹ Defined below.

hundreds of other Snowflake customer accounts, was targeted by an organized group of cyber criminals who infiltrated the third-party data storage environment and accessed certain database tables containing limited Ticketmaster customer data (the “Snowflake Environment”). This criminal enterprise, not Ticketmaster, caused the Data Incident alleged in the Complaint, but the steps Ticketmaster took ensured that its customers were not harmed by the Data Incident. Nor could the data at issue even give rise to any material risk of harm.

Although Plaintiffs’ Complaint assumes that the criminal actors’ breach of Snowflake creates liability for each defendant, the law recognizes that a data breach, by itself, is insufficient to sustain a lawsuit. That is exactly the case here with respect to the claims against Ticketmaster. Critically, the information involved in this case was principally comprised of customer names, phone numbers, and email addresses—all information that is publicly available—along with incomplete and protected payment card data. Moreover, Ticketmaster did not store card verification value (“CVV”) codes in the Snowflake Environment—which is necessary to use the cards—and Plaintiffs do not allege otherwise. In short, there was no information involved in the Data Incident that could cause Plaintiffs any harm or warrant any legitimate anxiety. Indeed, Plaintiffs’ failure to allege any identity theft or financial fraud in their Complaint—filed on May 19, 2025, nearly a year after the Data

Incident—is telling: there have been no confirmed instances of any such identity theft or fraud linked to the Data Incident at all.

Even so, Plaintiffs seek to convert the breach into gain. With threadbare allegations, Plaintiffs claim loss and blame Ticketmaster for the criminal actors' unlawful breach of Snowflake. But plausible facts are not advanced. A close examination of Plaintiffs' allegations about their individual experiences reveals a common thread: conclusory and thin assertions that fail to plausibly connect the Data Incident to any alleged (let alone actionable) injury.

Plaintiffs—ten Ticketmaster customers spanning five states—claim they gave Ticketmaster basic, non-sensitive contact information plus payment card data. They do not allege they gave Ticketmaster their dates of birth, driver's license numbers, passport information, or social security numbers. And some Plaintiffs fail to allege whether they even received notice that their data was potentially impacted by the Data Incident. Ultimately, none of them can tie any alleged harm to Ticketmaster.

Even taking all the allegations in the Complaint as true, Plaintiffs' claims fail for multiple reasons:

- No Injury-In-Fact or Cognizable Harm: This Court lacks subject matter jurisdiction because Plaintiffs' information could not be used by a bad actor, or is non-sensitive data, and Plaintiffs lack both injury-in-fact and legally cognizable injury;
- CCPA Claims: Plaintiffs' newly pleaded CCPA claims fail because the data did not constitute personal information under the statute and did not include the information necessary to actually use the payment cards

(i.e., Ticketmaster did not store the CVV codes in the Snowflake Environment);

- Breach of Contract Claims: Plaintiffs similarly cannot prevail on their breach claims because Ticketmaster did put security measures in place to protect the data, Plaintiffs cannot show any harm caused by the Data Incident, and Plaintiffs' requested relief is prohibited by contract;
- Negligence Claims: Because the data is unusable by any threat actor, and because the economic loss doctrine bars most Plaintiffs' negligence claims, they fail; and
- Various State Law Claims: Plaintiffs' state law claims fail for a variety of similar deficiencies.

For the reasons described more fully below, the Court should dismiss the Complaint in its entirety or strike portions of the Complaint identified below.

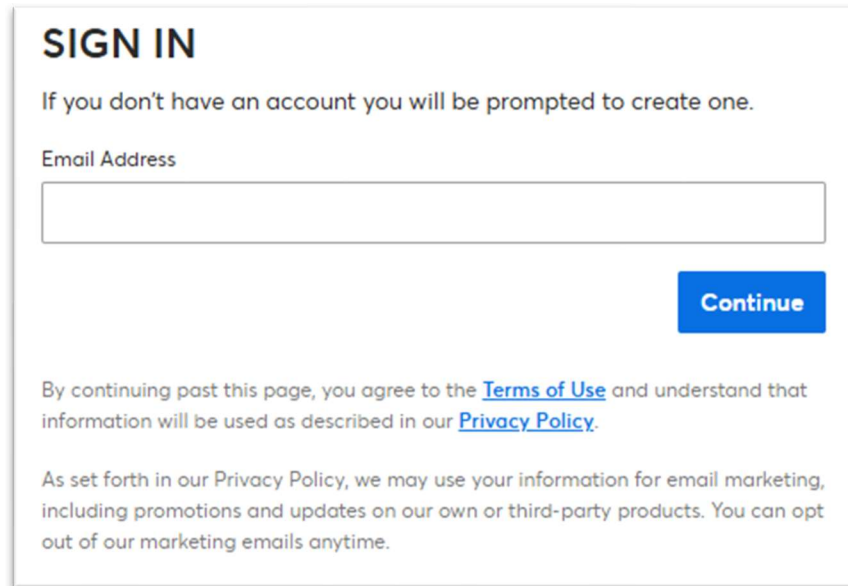
II. FACTUAL BACKGROUND²

Live Nation promotes, operates, and manages ticket sales while serving as the world's leading entertainment company. (Compl. ¶ 400.) Live Nation wholly owns Ticketmaster, L.L.C., a ticket distribution company specializing in entertainment events. (Compl. ¶¶ 15–16.)

² These facts are taken from Consumer Plaintiffs' operative Complaint and from facts within documents incorporated by reference in the Complaint. Lest there be any doubt, Ticketmaster disputes Plaintiffs' version of the facts and their complaint allegations. But consistent with the rules on a motion to dismiss, *Hunter v. Benefis Health Sys., Inc.*, No. 21-CV-92-GF-BMM, 2024 WL 664709, at *2 (D. Mont. Feb. 16, 2024), Ticketmaster accepts the facts as true for purposes of the motion.

A. Ticketmaster’s Privacy Policy and Terms of Use

Ticketmaster customers must sign into their Ticketmaster accounts to purchase tickets on the Ticketmaster website.³ To sign in, users must input their credentials and click a “Continue” button.^{4, 5}



³ Compl. ¶ 23, 60, 504; *see also* Declaration of William K. Whitner in Support of Ticketmaster’s Motion to Dismiss (Whitner Decl.), ¶ 8. Note, the Ticketmaster website—including all sign in pages—are incorporated by reference into the Complaint at Paragraphs 23, 60, and 504. *See Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005) (“The rationale of the ‘incorporation by reference’ doctrine applies with equal force to internet pages as it does to printed material. Just as a reader must absorb a printed statement in the context of the media in which it appears, a computer user necessarily views web pages in the context of the links through which the user accessed those pages.”).

⁴ Whitner Decl. ¶ 9.

⁵ The Ticketmaster “Sign in” webpage, including its graphics, changes from time to time; however, the relevant language cited within this webpage and relied upon in this Motion have remained the same at all relevant time periods.

Just below the “Continue” button, Ticketmaster informs users that “[b]y continuing past this page, you agree to the **Terms of Use** and understand that information will be used as described in our **Privacy Policy**.”⁶ Both “Terms of Use” and “Privacy Policy” are bold, colored blue for easy distinction, and hyperlinked to a separate webpage containing each document.⁷ The Complaint specifically references both the Terms of Use and the Privacy Policy. (Compl. ¶¶ 261, 262, 400–04.) And the Privacy Policy is expressly incorporated within the Terms of Use.⁸

The Privacy Policy states there are security measures Ticketmaster put in place to protect customers’ data, which depends on the type of information collected:⁹

⁶ *Id.* ¶¶ 8–10 (screenshot of the relevant sign-in page) (emphasis in original).

⁷ *Id.* ¶ 11.

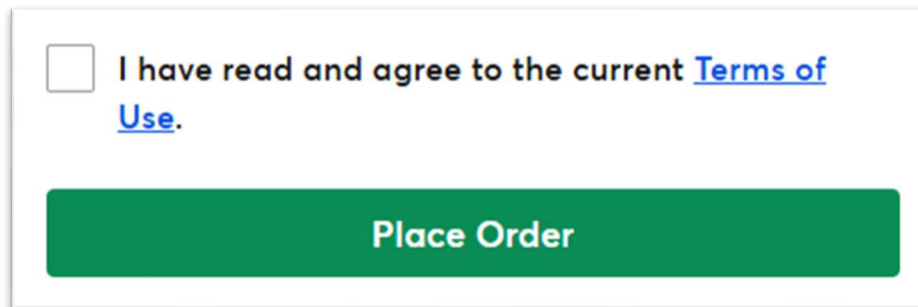
⁸ *Id.* ¶ 3, Ex. 1; *see also* Ticketmaster, *Terms of Use*, <https://help.ticketmaster.com/hc/en-us/articles/10468830739345-Terms-of-Use> (last updated July 2, 2021) (“Terms of Use”) (“Our Privacy Policy, Purchase Policy, and any other policies, rules, or guidelines that may be applicable to particular offers or features on the Site are also incorporated into the Terms. By visiting or using the Site, you expressly agree to these Terms, as updated from time to time.”).

⁹ Ticketmaster, *Privacy Policy*, <https://web.archive.org/web/20240226041015/https://privacy.ticketmaster.com/privacy-policy#contact-us> (archived Feb. 26, 2024) at “Looking After Your Information” (This is the same link cited in the Complaint (Compl. ¶ 400 n.161)); *see also* Whitner Decl. ¶ 2, Ex. 1.

LOOKING AFTER YOUR INFORMATION

We have security measures in place to protect your information. The security measures we use will depend on the type of information collected.

After signing in, users are taken to another webpage.¹⁰ Later, users must fill out payment and billing information and confirm the purchase by clicking a button titled “Place Order.”¹¹

A screenshot of a webpage section. At the top, there is a checkbox followed by the text "I have read and agree to the current [Terms of Use](#)." Below this text is a large green button with the white text "Place Order".

Just above the “Place Order” button, there is a checkbox stating, “I have read and agree to the current **Terms of Use**.”¹² Ticketmaster customers must check this checkbox prior to placing any order.¹³ Here, too, the referenced Terms of Use are

¹⁰ Whitner Decl. ¶ 12.

¹¹ *Id.* ¶ 12.

¹² *Id.* ¶¶ 12–13 (emphasis in original).

¹³ *Id.* ¶ 13.

bold, colored blue for easy distinction, and hyperlinked to a separate webpage containing the Terms.¹⁴

Each Plaintiff alleges they made Ticketmaster purchases, (Compl. ¶¶ 23, 28, 33, 38, 43, 47, 51, 55, 59, 64), meaning each Plaintiff also accepted Ticketmaster's Terms. The Terms clearly and unequivocally state:

WE DO NOT GUARANTEE THAT THE SITE WILL ALWAYS BE SAFE, SECURE, OR ERROR-FREE, OR THAT THE SITE WILL ALWAYS FUNCTION WITHOUT DISRUPTIONS, DELAYS, OR IMPERFECTIONS. WE ARE NOT RESPONSIBLE FOR THE ACTIONS OR INFORMATION OF THIRD PARTIES, AND YOU RELEASE US FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES.¹⁵

Thus, Ticketmaster expressly warns its customers of the risks associated with using its website. The Terms also include a provision that expressly limits its liability for unauthorized access to personal information:

IN NO EVENT WILL WE . . . BE RESPONSIBLE OR LIABLE TO YOU OR ANYONE ELSE FOR, AND YOU HEREBY KNOWINGLY AND EXPRESSLY WAIVE ALL RIGHTS TO SEEK, DIRECT, INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OF ANY TYPE . . . YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT WE WILL HAVE NO LIABILITY OR RESPONSIBILITY WHATSOEVER FOR . . . (c) ANY UNAUTHORIZED ACCESS TO OR USE OF OUR SECURE SERVERS AND/OR ANY AND ALL PERSONAL

¹⁴ *Id.* ¶ 13.

¹⁵ *See* Terms of Use § 14, *supra* note 8.

INFORMATION AND/OR FINANCIAL INFORMATION STORED THEREIN.¹⁶

B. Ticketmaster’s Security Measures and Snowflake

The Ticketmaster Privacy Policy further states that it collects customer “contact and billing information, such as [] name, street address, zip or post code, email, phone number and credit card.”¹⁷ Important for this case, the information involved in the Data Incident was **not** stored on Ticketmaster’s systems. (*See* Compl. ¶¶ 9, 401.) Instead, Ticketmaster engaged Snowflake to store customer data and to protect it.¹⁸ (*See* Compl. ¶¶ 9, 160, 270, 408, 411.) Critically, Plaintiffs admit Ticketmaster implemented a number of security measures when the data was stored in the Snowflake Environment to protect it from risk of harm including removing the CVV code, (*see* Compl. ¶¶ 202, 473), and hashing the payment card data, (*see* Compl. ¶ 457), rendering it both unusable and unreadable to unauthorized third parties in its garbled form. Plaintiffs also allege that some of the data included just the “last four digits of” the card number. (Compl. ¶ 473.)

¹⁶ *Id.* § 15.

¹⁷ Privacy Policy, *supra* note 9.

¹⁸ The Complaint incorporates by reference various Snowflake websites that describe Snowflake’s security services at Paragraphs 270–274. *See also* Whitner Decl. ¶ 4, Ex. 3; Snowflake, *Snowflake Security Hub*, <https://www.snowflake.com/en/why-snowflake/snowflake-security-hub/> (last visited June 16, 2025) (“Snowflake services and accounts are designed for security, lowering the risk of vulnerabilities and breaches with features that help customers configure comprehensive levels of security for their data and users.”).

In May 2024, Ticketmaster and over 100 other Snowflake customers discovered a sophisticated threat actor was systematically targeting and potentially exfiltrating customer data hosted by Snowflake (the “Snowflake Incidents”) (specifically identified as the “Data Incident” when referring to the Ticketmaster data storage environment).¹⁹ A third-party security firm, Mandiant, then advised many Snowflake customers of potentially unauthorized access to their Snowflake environments.²⁰

Like all of Ticketmaster’s vendors who may have access to or store its customers’ information, Ticketmaster evaluated Snowflake in accordance with its Third-Party Risk Management (“TPRM”) Program.²¹ When the Data Incident occurred, Ticketmaster had been a Snowflake customer for several years. (*See* Compl. ¶ 277.) Throughout that time, Snowflake had repeatedly represented that it would (a) monitor the Snowflake environment in real-time, including with respect

¹⁹ *See* Compl. ¶¶ 9, 158–61, 163, 311, which incorporate by reference the “Mandiant Report;” Mandiant, *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion, Google Cloud* (June 10, 2024), <https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion> (cited to hereinafter as “Mandiant Report”); *see also* Whitner Decl. ¶ 5, Ex. 4.

²⁰ *Id.*

²¹ *See* Compl. ¶ 400 & n.160, which incorporates by reference Live Nation’s 2024 Annual Report; Live Nation Entertainment, Inc., Annual Report (Form 10-K) at 17–18 (Feb. 22, 2024), <https://investors.livenationentertainment.com/sec-filings/annual-reports/content/0001335258-24-000017/0001335258-24-000017.pdf>; *see also* Whitner Decl., ¶ 6, Ex. 5.

to suspicious access attempts, and (b) report suspected data security incidents to its customers. (*See* Compl. ¶¶ 3, 270–73, 407; Compl. ¶ 3 n.2.)

In response to the Data Incident, Ticketmaster immediately launched an investigation.²² In addition to engaging outside counsel and leveraging its considerable internal cybersecurity resources, Ticketmaster was supported by an industry-leading cybersecurity forensics firm.²³ Ticketmaster’s current understanding is that the threat actor took steps similar to the tactics, techniques, and procedures used in recent attacks perpetrated on many of Snowflake’s other customers. Many victims of the Snowflake Incidents had credentials stolen from their third-party contractors. (Compl. ¶ 285.)

On May 23, 2024, Ticketmaster determined that some personal information regarding Ticketmaster customers may have been impacted and began focusing its efforts on timely identifying and notifying potentially impacted individuals out of an abundance of caution. (Compl. ¶¶ 450, 464.) This resulted in Ticketmaster over-

²² *See* Compl. ¶ 202 & n.79 which incorporates by reference Ticketmaster’s press release concerning the Data Incident; Ticketmaster, *Ticketmaster Data Security Incident*, <https://help.ticketmaster.com/hc/en-us/articles/26110487861137-Ticketmaster-Data-Security-Incident> (last visited Jun. 16, 2025); *see also* Whitner Decl. ¶ 7, Ex. 6.

²³ *Id.*

notifying customers because not all persons who were notified were potentially at risk.²⁴

C. The Data Potentially Impacted

The Data Incident largely involved non-sensitive contact information and information about customer transactions.²⁵ This non-sensitive contact information included items such as names, phone numbers, email addresses, and physical addresses.²⁶

The Data Incident also involved payment card information that was “hashed” or limited to “the last four digits” of each payment card. (Compl. ¶¶ 202, 472–73.) Plaintiffs do not allege the CVV code associated with any of their payment cards was included in the Data Incident. (Compl. ¶¶ 202, 472–73.) This information presents minimal to no risk to any customer because, even in the hands of a threat actor, it cannot be used in its stored, garbled, and/or incomplete form. Importantly, Plaintiffs also never allege, let alone explain, how the credit card data would be usable without the CVV code. Instead, they cite to a single general article that talks about the potential risk of storing credit card data in hashed form. (Compl. ¶ 461.)

²⁴ (ECF. No. 419-9 (containing several Plaintiffs’ Data Incident notification letters—which Plaintiffs agree are incorporated by reference in the Complaint at ¶¶ 23, 38, 43, 47, 55, 59, and 64 (*see* ECF No. 443)—and stating the Data Incident “*may have involved your personal information*”).)

²⁵ *Ticketmaster Data Security Incident*, *supra* note 22.

²⁶ *Id.*

D. Plaintiffs and Their Lawsuits

Plaintiffs’ specific allegations often lack a clear description of any harm they suffered. Plaintiffs Eric Anderson²⁷, Charles Fitzgerald²⁸, Susie Garcia-Nixon²⁹, Valerie Lozoya³⁰, LaVonne Madden³¹, Jolinda Murphy³², Lauren Neve³³, Molly O’Hara³⁴, Dekima Thomas³⁵, and Christina Xian³⁶ (collectively, “Plaintiffs”) are purported Ticketmaster customers whose data was allegedly included within the Data Incident. (Compl. ¶¶ 23–68.)

While seven Plaintiffs³⁷ allegedly received data breach notification letters from Ticketmaster, three Plaintiffs³⁸ fail to allege they received a notice for the Data Incident. (Compl. ¶¶ 23–68.)

²⁷ Plaintiff Anderson is a resident of New York.

²⁸ Plaintiff Fitzgerald is a resident of New York.

²⁹ Plaintiff Garcia-Nixon is a resident of California.

³⁰ Plaintiff Lozoya is a resident of California.

³¹ Plaintiff Madden is a resident of Montana.

³² Plaintiff Murphy is a resident of Montana.

³³ Plaintiff Neve is a resident of California.

³⁴ Plaintiff O’Hara is a resident of Massachusetts.

³⁵ Plaintiff Thomas is a resident of Washington, D.C.

³⁶ Plaintiff Xian is a resident of California.

³⁷ Plaintiffs Anderson, Lozoya, Madden, Murphy, O’Hara, Thomas, and Xian.

³⁸ Plaintiffs Fitzgerald, Garcia-Nixon, and Neve.

Plaintiffs allegedly shared their “name, address, email, phone number, payment card information, and transaction information” with Ticketmaster. (Compl. ¶¶ 23, 28, 33, 38, 43, 47, 51, 55, 60, 64.) However, some of the data that was shared with Ticketmaster was not included in the data stolen from the Snowflake Environment, including the CVV code for the credit cards.³⁹ And the Complaint does not specify which of Plaintiffs’ information *was* potentially included in the Data Incident, only that Plaintiffs shared certain information with Ticketmaster.

Despite the security measures in place to protect payment card information (e.g., not storing CVV codes) and the lack of sensitive information involved, Plaintiffs identify several harms allegedly derived from the Data Incident.

Five Plaintiffs⁴⁰ allege fraudulent activity on their payment cards. (Compl. ¶¶ 24, 29, 34, 39, 65.) Plaintiff Anderson, for example, states “[he] experienced fraudulent payment card activity” and “had several unauthorized charges, prompting the bank to close his card and issue a replacement.” (Compl. ¶ 24.) But neither Plaintiff Anderson nor any other Plaintiff alleges the payment cards potentially impacted by any alleged fraudulent conduct were also used to make Ticketmaster purchases. And no Plaintiff states they personally paid for the alleged fraudulent charges, nor do they discuss whether the card company reimbursed them.

³⁹ *Ticketmaster Data Security Incident*, *supra* note 22.

⁴⁰ Plaintiffs Anderson, Fitzgerald, Garcia-Nixon, Lozoya, and Xian.

Three Plaintiffs⁴¹ generally claim they were notified that their information was found on the dark web. (Compl. ¶¶ 25, 30, 56.) Plaintiff Anderson, for example, states “[he] was informed by his credit card company that his personal information was found on the dark web.” (Compl. ¶ 25.) But these Plaintiffs do not identify what information was on the dark web, whether their data included within the Data Incident was found on the dark web, and whether the Data Incident caused their information to appear on the dark web. In short, none of these Plaintiffs allege this purported harm was tied to the Data Incident in any way.

Six Plaintiffs⁴² allegedly received spam calls and text messages, (Compl. ¶¶ 25, 40, 48, 52, 56, 61), and all Plaintiffs generally allege emotional damages and the following additional alleged harms:

overpayment for services [they] did not receive; the unauthorized use of his stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of [their] Personal Information; invasion of [their] privacy; and emotional distress and anxiety resulting from the theft of [their] Personal Information and responding to identity theft.

(Compl. ¶¶ 26, 31, 36, 41, 45, 49, 53, 57, 62, 67.)

⁴¹ Plaintiffs Anderson, Fitzgerald, and O’Hara.

⁴² Plaintiffs Anderson, Lozoya, Murphy, Neve, O’Hara, and Thomas.

III. PROCEDURAL BACKGROUND

Beginning May 2024, various consumer plaintiffs, including these Plaintiffs, filed several federal lawsuits against Ticketmaster and other entities asserting claims arising from the Snowflake Incidents. (ECF No. 1 at 7.) On July 29, 2024, a plaintiff in one of these actions filed a motion before the United States Judicial Panel on Multidistrict Litigation (the “JPML”) asking the JPML to transfer and centralize the numerous actions arising from the Data Incident, pursuant to 28 U.S.C. § 1407. (*Id.* at 1.)

On October 8, 2024, the JPML issued its Transfer Order finding centralization in the District of Montana was appropriate because the district had capacity, many of the actions at issue were already pending in the district, and multiple parties selected the district as their first or second choice or were unopposed to the district. (*Id.* at 4–5.) The JPML thus consolidated the actions and transferred them to this Court. (*Id.*)

Plaintiffs filed a Representative Class Action Complaint on February 3, 2025, (ECF No. 320), which Plaintiffs amended on April 14, 2025, (ECF No. 395). Plaintiffs and Ticketmaster filed a Joint Motion to Stay Proceedings on February 25, 2025, which sought to stay proceedings to allow the parties to pursue mediation, which proved unsuccessful. (ECF No. 352.)

On May 15, 2025, the parties filed a Joint Status Report, asking the Court to lift the stay and provide a proposed schedule to govern the case going forward. (ECF No. 416.) Plaintiffs filed their Third Amended Representative Class Action Complaint on May 19, 2025. (ECF No. 427.)

IV. LEGAL STANDARD

A. Rule 12(b)(1)

Rule 12(b)(1) requires dismissal of a complaint for lack of subject matter jurisdiction. This jurisdictional attack can be either facial or factual. *White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000). “A ‘facial’ attack asserts that a complaint’s allegations are themselves insufficient to invoke jurisdiction, while a ‘factual’ attack asserts that the complaint’s allegations, though adequate on their face to invoke jurisdiction, are untrue.” *Courthouse News Serv. v. Planet*, 750 F.3d 776, 780 n.3 (9th Cir. 2014) (citing *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004)). Ticketmaster asserts a facial attack for lack of Article III standing.

B. Rule 12(b)(6)

“Dismissal proves appropriate under Rule 12(b)(6) where the complaint fails to state a claim upon which relief can be granted.” *Est. of Rogel v. City of Bozeman*, No. 24-cv-034-BU-BMM, 2025 WL 1249223, at *1 (D. Mont. Apr. 30, 2025) (citing *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008)). To survive dismissal, Plaintiffs must allege facts that demonstrate a “plausible” basis

for relief. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007). “Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). “A claim proves plausible on its face when ‘the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.’” *Est. of Rogel*, 2025 WL 1249223, at *2 (citing *Iqbal*, 556 U.S. at 678). A complaint offering only “an unadorned, the-defendant-unlawfully-harmed-me accusation” or “labels and conclusions” fails to meet this standard. *Iqbal*, 556 U.S. at 678.

“[P]lausibility pleading standards are especially important in cases like this one, where the Defendant faces the ‘potentially enormous expense of discovery’ if the Court denies this motion to dismiss.” *Razuki v. Caliber Home Loans, Inc.*, No. 17-CV-1718-LAB, 2018 WL 6018361, at *2 (S.D. Cal. Nov. 15, 2018) (quoting *Twombly*, 550 U.S. at 559).

C. Rule 12(f)

Under Rule 12(f), “[t]he court may strike from a pleading an insufficient defense or any redundant, immaterial, impertinent, or scandalous matter.” FED. R. CIV. P. 12(f). “[T]he function of a 12(f) motion to strike is to avoid the expenditure of time and money that must arise from litigating spurious issues by dispensing with those issues prior to trial.” *Cintron v. Title Fin. Corp.*, No. CV 17-108-M-DLC,

2018 WL 692936, at *1 (D. Mont. Feb. 1, 2018) (citing *Sidney–Vinstein v. A.H. Robins Co.*, 697 F.2d 880, 885 (9th Cir. 1983)).

Relevant here, “[i]mmaterial matter is that which has no essential or important relationship to the claim for relief or the defenses being pleaded.” *United States v. Rhodes*, No. CV 21-110-M-DLC-KLD, 2023 WL 129859, at *1 (D. Mont. Jan. 9, 2023) (citing *Fantasy, Inc. v. Fogerty*, 984 F.2d 1524, 1527 (9th Cir. 1993)), *rev’d on other grounds*, 510 U.S. 517 (1994)), *aff’d*, No. CV 21-110-M-DLC, 2023 WL 197088 (D. Mont. Jan. 17, 2023). “Impertinent matter consists of statements that do not pertain, and are not necessary, to the issues in question.” *Id.* If the Court chooses not to dismiss Plaintiffs’ claims, it may still strike various individual allegations, including any of Plaintiffs’ alleged harms that the Court finds unrecoverable as a matter of law. *United States v. Hossain*, No. 22-16085, 2023 WL 5319262, at *1 (9th Cir. Aug. 18, 2023) (where the Ninth Circuit affirmed a “district court’s order granting the government’s motion to strike [plaintiff’s] claim for lack of Article III standing”); *Flynn v. FCA US LLC*, No. 15-CV-0855-MJR-DGW, 2016 WL 5341749, at *3 (S.D. Ill. Sept. 23, 2016) (finding Plaintiffs lack standing on a subset of their Article III injuries, including “risk of injury or death and the fear of that injury”).

D. Applicable Choice of Law

For the majority of the specific arguments in this Motion, the Court can dismiss Plaintiffs’ claims without addressing the broader choice-of-law issues. However, Plaintiffs do not reside in a common forum. Rather they are from California, Massachusetts, Montana, New York, and Washington, D.C. (Compl. ¶¶ 23, 28, 33, 38, 43, 47, 51, 55, 59, 64.) Except for the statutory claims, no Plaintiff identifies the law governing their common law claims (*e.g.*, breach of contract, negligence). While the basics of *pleading* a breach of contract claim or a negligence claim share a common core across states,⁴³ the substance of whether a claim will lie (on issues like damages or duty, or defenses) can be outcome determinative and do differ across forums.⁴⁴ Accordingly, Ticketmaster preliminarily raises the choice-of-law issues now.

To that end, Montana’s approach to choice of law (applicable here) depends on the type of claim. In general, “Montana uses the approach from the Restatement (Second) of Conflict of Laws to resolve disputes over which state’s substantive law applies to a particular action.” *Talbot v. Ainuu*, No. CV-23-66-BU-BMM, 2024 WL 896370, at *2 (D. Mont. Mar. 1, 2024) (citing *Buckles v. BH Flowtest, Inc.*, 476 P.3d 422, 424 (Mont. 2020)). But because Montana has an express statutory provision

⁴³ See, *e.g.*, *infra* notes 55, 68.

⁴⁴ See, *e.g.*, *infra* note 67.

governing applicable law for contract disputes, Mont. Code Ann. § 28-3-102, it controls. Under the statute, “[a] contract is to be interpreted according to the law and usage of the place where it is to be performed or, if it does not indicate a place of performance, according to the law and usage of the place where it is made.” *Id.* Using each Plaintiff’s residence as a proxy for where they consented to the agreement and thus where it was made, *see Corp. Air v. Pratt & Whitney Canada Corp.*, No. CV 08-33-BLG-RFC, 2009 WL 10701737, at *3 (D. Mont. Aug. 21, 2009), means the state of each Plaintiff’s residence (for purposes of this motion to dismiss) should govern their contract claim.

The same result—*i.e.*, each Plaintiff’s claims is governed on this motion by their alleged residence—applies to Plaintiffs’ tort claims, too, but under a different analysis. Namely, the general principles outlined in §§ 6(2) and 145 of the Restatement govern. *Buckles*, 476 P.3d at 425. Under the combined Restatement analysis, courts look to factors like “where the injury occurred,” “the place where the conduct causing the injury occurred,” “the domicil, residence, nationality, place of incorporation and place of business of the parties,” and “the place where the relationship, if any, between the parties is centered.” Restatement (Second) Conflict of Laws § 145(2)(a)-(d). Here again, that all leads (at this stage) to each Plaintiff’s residence since each state has an interest in regulating purchases made within their state.

That being said, Ticketmaster recognizes that parsing choice-of-law issues for the Court can be cumbersome at this stage. Thus, in the main, Ticketmaster's pleading challenges on the common law claims are the same across the jurisdictions and are presented together. To ease the Court's analysis, Ticketmaster specifies when an argument applies only to a given Plaintiff or a limited group of Plaintiffs based on the applicable law.

V. ARGUMENT

Plaintiffs' claims all suffer from a host of legal and factual issues, the most pressing of which are a lack of harm and an inability to show that any harm could arise from the theft of incomplete and unusable payment card information.

A. Plaintiffs Cannot Establish Article III Standing

Even taking all of Plaintiffs' allegations as true, they have a standing problem as they have not been harmed and, even if they were, their alleged harms are not traceable to the Data Incident.

Unfortunately, data breaches are common. *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 365 (M.D. Pa. 2015) (finding "data breaches [have] unfortunately become common occurrences in the modern world"). Indeed, "[t]here are only two types of companies left in the United States, according to data security experts: 'those that have been hacked and those that don't know they've been hacked.'" *Id.* at 360 (citation omitted). And while many of Plaintiffs' claimed injuries are not

recoverable by law, even if they were, these injuries were likely caused by a source other than the Data Incident. The law, therefore, requires a plaintiff to plead—consistent with their Rule 11 obligations—that their harms were caused by the breach and explain how.

“[T]hose who seek to invoke the jurisdiction of the federal courts must satisfy the threshold [sic] requirement imposed by Article III of the Constitution by alleging an actual case or controversy.” *City of Los Angeles v. Lyons*, 461 U.S. 95, 101 (1983); *Montana Wildlife Fed’n v. Bernhardt*, No. 4:18-CV-69-BMM, 2021 WL 4865257, at *1 (D. Mont. June 21, 2021) (“Plaintiffs must establish that they possess standing to invoke the Court’s jurisdiction.”) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 559–60 (1992)). “[T]o satisfy Article III’s standing requirements, a plaintiff must show (1) it has suffered an ‘injury in fact’ that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.” *Friends of the Earth, Inc. v. Laidlaw Env’t Servs., Inc.*, 528 U.S. 167, 180-81 (2000) (citations omitted).⁴⁵

⁴⁵ Ticketmaster admits that the law in this space is fractured. Where it knows of controlling Ninth Circuit or Supreme Court precedent, it has cited it. Where such law is absent, it has cited the law favorable to its position while here acknowledging that issue-by-issue, this Court (or Plaintiffs) could find contrary non-binding district court (or out-of-Circuit) authority. Ticketmaster suggests to the Court that the best

In addition to Article III’s injury-in-fact requirement, Plaintiffs must also establish that their injuries are legally cognizable, meaning there must be an actual injury. *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (2013). Plaintiffs in data breach cases, like Plaintiffs here, often fail this test. *Johnson v. Yuma Reg’l Med. Ctr.*, No. CV-22-01061-PHX-SMB, 2024 WL 4803881, at *1-2 (D. Ariz. Nov. 15, 2024) (finding plaintiffs failed to plead cognizable damages under several causes of action, including damages allegations of diminution of value, lost time, emotional distress, spam, risk of fraud, and delay in notice).⁴⁶ This is because, “the mere misappropriation of personal information does not establish compensable damages.”

way to work through the issues is to parse them (as many courts have done) through the lens of the Supreme Court’s guidance in cases like *TransUnion* and *Clapper*.

⁴⁶ The cognizable injury requirement is common across all jurisdictions implicated by the complaint. *See, e.g., Reidy v. UMass Mem’l Med. Ctr., Inc.*, No. 2085-CV-01101, 2021 WL 6777622, at *2 (Mass. Super. Ct. June 17, 2021) (finding that plaintiff’s “assertions [were], at best, abstract concerns about possible future impairments of his rights as a patient, without actual damages, and, as such, [were] insufficient to state his claims against [defendant] for negligence, breach of fiduciary duty, breach of contract, and violation of statutes prohibiting invasion of right to privacy and breach of confidentiality.”); *Caronia v. Philip Morris USA, Inc.*, 5 N.E.3d 11, 14 (N.Y. 2013) (“A threat of future harm is insufficient to impose liability against a defendant in a tort context.”); *Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 708 (D.C. 2009) (“To maintain an action for negligence, a plaintiff must allege more than speculative harm from defendant’s allegedly negligent conduct.”); *Tarter v. Throne L. Off., P.C.*, No. 17-CV-123-BLG-SPW, 2019 WL 462985, at *5 (D. Mont. Feb. 6, 2019) (“Speculative damages not clearly ascertainable are not recoverable.”).

Pruchnicki v. Envision Healthcare Corp., 845 F. App’x 613, 614–15 (9th Cir. 2021) (quotation marks and citations omitted).

1. *Plaintiffs’ Claimed Injuries Do Not Confer Standing*

Ninth Circuit precedent instructs courts to dismiss no-injury data breach cases where, as here, the plaintiff “fail[s] to adequately allege damages stemming from a data breach.” *Id.* at 614. Here, because the payment card information in the Snowflake Environment was not usable, Plaintiffs struggle to show any concrete harm that they suffered. Courts throughout this Circuit find the types of damages that are actually asserted by Plaintiffs, such as time lost and emotional damage from alleged breaches, are insufficient to plead Article III standing. *See, e.g., Morales v. Conifer Revenue Cycle Sols., LLC*, No. 2:23-CV-01987-AB-AGR, 2025 WL 1096396, at *4 (C.D. Cal. Mar. 31, 2025) (rejecting appeals to identity theft, lost time, emotional damages, diminished value of personal identifiable information, and an increase in spam calls). Here, too, most Plaintiffs’ alleged harms fail to plead what Circuit law requires to convey standing.

Spam calls and messages. Six Plaintiffs⁴⁷ seek damages for spam calls and text messages (Compl. ¶¶ 25, 40, 48, 52, 56, 61); however, these claimed injuries do not confer Article III standing. “Spam calls, texts, and e-mails have become very

⁴⁷ Including Plaintiffs Anderson, Lozoya, Murphy, Neve, O’Hara, and Thomas.

common in this digitized world, and a number of courts have declined to confer standing when considering an increase in spam communications.” *McCombs v. Delta Grp. Elecs., Inc.*, 676 F. Supp. 3d 1064, 1074 (D.N.M. June 9, 2023); *In re Illuminate Educ. Data Sec. Incident Litig.*, No. SACV 22-1164 JVS (ADSx), 2023 WL 3158954, at *3 (C.D. Cal. Apr. 19, 2023) (finding “[r]eceipt of spam, absent any other injury, is insufficient to establish an injury for the purposes of standing”); *see also Black v. IEC Grp., Inc.*, No. 1:23-CV-00384-AKB, 2024 WL 3623361, at *6 (D. Idaho July 30, 2024) (“Courts generally reject that a plaintiff’s receipt of spam messages is an injury sufficient to confer standing.”).

Threatened risk of identity theft. All Plaintiffs allege a “substantial risk of identity theft” simply because the Data Incident occurred. (Compl. ¶¶ 26, 31, 36, 41, 44, 49, 53, 57, 62, 67, 480.) But it is bedrock law that “the mere risk of future harm, standing alone, cannot qualify as a concrete harm” for Article III standing purposes. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 436 (2021). In a post-*TransUnion* world, many courts recognize that “in light of *TransUnion*’s rejection of risk of harm as a basis for standing for damages claims” there is no Article III standing based on future harm. *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1054 & n.15 (N.D. Cal. 2022) (granting motion). “[T]he Supreme Court is clear that where a risk of future harm has not yet materialized, the ‘plaintiffs’ argument for standing for their damages claims based on an asserted risk of future harm is unavailing.”

Bock v. Washington, 33 F.4th 1139, 1145 (9th Cir. 2022) (citing *TransUnion*, 594 U.S. at 437). Thus, Plaintiffs’ risk of future harm is not an injury that grants them standing, and that theory of harm should be dismissed.

Lost Value of Personally Identifiable Information (“PII”). So too do Plaintiffs lack standing to claim that the value of their PII has diminished. Plaintiffs summarily state their PII “has inherent value,” Compl. ¶ 483, without alleging any facts to support whether the PII *actually* lost value, which is required as a matter of law. *See, e.g., Pruchnicki*, 845 F. App’x at 614–15 (finding no Article III standing for that plaintiff’s lost value of PII injury because “[a]lthough the studies cited by [plaintiff] establish that personal information may have value in general, [plaintiff] failed to adequately allege that [*their*] personal information actually lost value”).

Plaintiffs fail to allege basic facts such as the dollar amount attributable to their PII, whether they even intended to sell their PII, or whether they were precluded from using it in any subsequent, for-value transactions, making any lost value claim insufficient as a matter of law. *See, e.g., Hemphill v. Horne, LLP*, No. 3:24-CV-178-KHJ-ASH, 2025 WL 837007, at *7 (S.D. Miss. Mar. 10, 2025) (finding “[Plaintiffs] also fail to plead a concrete injury based on the diminished value of their PII” because Plaintiffs failed to plead actual misuse of their data as a result of the data breach); *Capiau v. Ascendum Mach., Inc.*, No. 3:24-CV-00142-MOC-SCR, 2024 WL 3747191, at *6 (W.D.N.C. Aug. 9, 2024) (finding “Plaintiff lacks standing

to pursue claims predicated on the diminished value of his PII” because he failed to plead “facts suggesting that his PII’s value did in fact decrease due to the [data] breach”). Thus, Plaintiffs have alleged no diminution in value of their PII sufficient to confer standing.

Lost Time Spent Investigating, Credit Monitoring, & Emotional Distress.

The same goes for Plaintiffs’ “lost time,” monitoring expenses, and emotional distress theories of alleged harm. Plaintiffs specifically allege they “suffered injury in the form of lost time and resources mitigating against the risk of identity theft and emotional distress arising from the risk of identity theft.” (Compl. ¶ 480.) Plaintiffs also seek to recover “time and expenses spent obtaining credit monitoring services” as part of these mitigation efforts. (Compl. ¶¶ 26, 31, 35, 41, 48, 53, 57, 62.) But as the Eighth Circuit explained, “[b]ecause plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury.” *In re SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017) (citing *Clapper*, 568 U.S. at 416 (plaintiffs “cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending”))).

The Eleventh Circuit agrees: “[e]vidence of a mere data breach does not, standing alone, satisfy the requirements of Article III standing.” *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021). So, where a would-

be plaintiff “voluntarily spen[ds] time” in response to a data breach without plausibly alleging specific facts moving the breach beyond an “insubstantial, non-imminent risk of identity theft,” he has not alleged standing. *Id.* at 1345.

Here, Plaintiffs often do not allege that their personal information was even part of the Data Incident—and only some of them allegedly received a data breach notice. (See Compl. ¶¶ 23, 38, 43, 47, 55, 59, 64.) But even if it was, courts have concluded this is insufficient to create lost time or fear-based Article III standing, or to convert monies they spent on credit monitoring into such standing, particularly where (as here) social security numbers were not involved.

For example, in *Whalen v. Michaels Stores, Inc.*, 689 F. App’x 89, 90 (2d Cir. 2017), where a plaintiff’s credit card number was stolen as part of a data breach, but she promptly cancelled her credit card “and no other [PII]—such as her birth date or Social Security number—[was] alleged to have been stolen,” the court found the plaintiff failed to allege “how she [could] plausibly face a threat of future fraud” and thus standing was lacking.⁴⁸ Similarly, in *Travis v. Assured Imaging LLC*, No. CV-

⁴⁸ Plaintiffs may seek to respond to *Whalen* by citing to *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018), where credit card information was stolen and standing was found. But in doing so, Plaintiffs would have to acknowledge critical differences in the incidents, including that here (and unlike in *Zappos*) the payment card information was hashed (*see* Compl. ¶ 457), and that in *Zappos* much more information was stolen, including *passwords*, as the threat actor “allegedly stole the names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information of more than 24 million Zappos customers.” *Id.* at 1023.

20-00390-TUC-JCH, 2021 WL 1862446, at *10 (D. Ariz. May 10, 2021), the court held that “emotional distress, anxiety and ‘lack of privacy’” from a ransomware attack was insufficient to confer Article III standing. And, in *Ables v. Brooks Bros. Grp.*, No. CV 17-4309-DMG (EX), 2018 WL 8806667, at *7 (C.D. Cal. June 7, 2018), the court held “[i]n the absence of increased risk of future harm, neither time nor money expended by Ables to mitigate a hypothetical risk confers standing.”

So too for these Plaintiffs. They have not alleged plausible facts demonstrating an imminent risk of identity fraud.

Information on the Dark Web. Three Plaintiffs⁴⁹ allege their PII has been found on the dark web. (Compl. ¶¶ 25, 30, 56.) But courts routinely find lack of injury for this type of harm as well. *Zynga, Inc.*, 600 F. Supp. 3d at 1039, 1055 (finding no standing despite complaint allegations that “the affected users’ PII have been sold or otherwise published on the dark web”); *see also Liao v. Weee! Inc.*, No. 23-CV-1177-PAE, 2024 WL 729259, at *4 (S.D.N.Y. Feb. 22, 2024) (noting that exposure of information on the dark web that could not be used to steal a person’s identity will not support an Article III injury-in-fact).

Invasion of Privacy/Unauthorized Use. Although all Plaintiffs allege invasion of privacy, they must also plead this harm was “caused by the disclosure of

⁴⁹ Including Plaintiffs Anderson, Fitzgerald, and O’Hara.

or intrusion upon matters of a kind that would be ‘highly offensive to a reasonable person.’” *Zynga, Inc.*, 600 F. Supp. 3d at 1049 (citing Restatement (Second) of Torts § 652D). Plaintiffs fail to do so and instead admit that their payment card information was hashed, and they do not allege the CVV code associated with the credit card was included in the Data Incident.

Non-sensitive data such as name, email address, phone number, and address are not highly offensive. *Zynga, Inc.*, 600 F. Supp. 3d at 1049 (finding “basic contact information, including one’s email address, phone number, or Facebook or Zynga username” was not highly offensive). The *Zynga, Inc.* court reasoned there is “an insufficient fit between the loss of information alleged here and the common law privacy tort[] of private disclosure of private facts” because plaintiff’s exposed data “is designed to be exchanged to facilitate communication and is thus available through ordinary inquiry and observation.” *Id.* at 1049–50. And the lack of the CVV code and hashed payment card data that masks the actual number and renders it unusable is also not offensive because it cannot plausibly cause fraudulent use of a payment card. *Cf. Cooper v. Bonobos, Inc.*, No. 21-CV-854-JMF, 2022 WL 170622, at *4 (S.D.N.Y. Jan. 19, 2022) (dismissing plaintiff’s complaint where “the hack did not compromise his full credit card number; it merely compromised the last four digits of his credit card, and he does not allege—let alone allege plausibly—that criminals could use that limited information to cause him harm”).

Benefit of the Bargain. Plaintiffs’ last addition (in their latest amendment) is to claim that they have standing based on a benefit of the bargain theory. That theory fails, too, and *Jackson v. Loews Hotels, Inc.*, discussed below, explains why. No. ED18-CV-827-DMG-JCX, 2019 WL 6721637, at *2 (C.D. Cal. July 24, 2019).

The gist of Plaintiffs’ theory is that some portion of the fees they paid Ticketmaster can be considered an in-kind trade for perfect data security. (Compl. ¶¶ 23, 28, 33, 38, 43, 47, 51, 55, 60, 64, 429-30, 445–46, 482.) They point to the company’s website and its Privacy Policy and Terms of Use. (Compl. ¶¶ 261–62, 400–09.) But in *Jackson*, plaintiffs sought to base standing on the same theory which the court rejected because the Privacy Policy there, as does the Privacy Policy here, negated any such reliance:

The Privacy Policy states that “[t]he personal information collected from users online ... is stored by Loews ... on databases protected through a combination of physical and electronic access controls, firewall technology and other reasonable security measures.” *Loew’s Hotels Privacy Policy*, <https://www.loewshotels.com/privacy-policy> at “Protecting Personal Information” (last visited April 18, 2019). It continues, however, to warn customers that “[n]evertheless, such security measures cannot prevent all loss, misuse or alteration of personal information and Loews is not responsible for any damages or liabilities relating to any such incidents to the fullest extent permitted by law.” *Id.* It also states that “no security system or system of transmitting data over the Internet can be guaranteed to be entirely secure. Use of the Services and related applications and transmission of data is at the user’s own risk. *Id.*”

Id. at *2. “Accordingly, Plaintiff has not established that she lost the benefit of any bargain sufficient to confer Article III standing.” *Id.*

Just as *Jackson* warned that it was *not* promising absolute data security, so too did Ticketmaster. First, the Privacy Policy stated that Ticketmaster would have “security measures in place to protect your information,”⁵⁰ which they did—including by not storing CVV codes in the Snowflake Environment. In addition, the Terms of Use specifically stated that:

WE DO NOT GUARANTEE THAT THE SITE WILL ALWAYS BE SAFE, SECURE, OR ERROR-FREE, OR THAT THE SITE WILL ALWAYS FUNCTION WITHOUT DISRUPTIONS, DELAYS, OR IMPERFECTIONS. WE ARE NOT RESPONSIBLE FOR THE ACTIONS OR INFORMATION OF THIRD PARTIES, AND YOU RELEASE US FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES.⁵¹

As *Jackson* disclaimed liability for the invasive acts of others and advised its customers that they proceeded at their own risk, Ticketmaster did the same:

IN NO EVENT WILL WE . . . BE RESPONSIBLE OR LIABLE TO YOU OR ANYONE ELSE FOR, AND YOU HEREBY KNOWINGLY AND EXPRESSLY WAIVE ALL RIGHTS TO SEEK, DIRECT, INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OF ANY TYPE . . . YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT WE WILL HAVE NO LIABILITY OR RESPONSIBILITY WHATSOEVER FOR . . . (c) ANY UNAUTHORIZED ACCESS TO OR USE OF OUR SECURE SERVERS AND/OR ANY AND ALL PERSONAL INFORMATION AND/OR FINANCIAL INFORMATION STORED THEREIN.⁵²

⁵⁰ Privacy Policy, *supra* note 9.

⁵¹ Terms of Use § 14, *supra* note 8.

⁵² *Id.* § 15.

Thus, similar to *Jackson*, Plaintiffs’ benefit of the bargain theory fails here as well.

Other courts have likewise rejected the benefit of the bargain theory where a plaintiff, like these Plaintiffs, cites to stray references to safety on a website or Privacy Policy without a corresponding allegation that the plaintiff at issue actually read the passage asserted. *See, e.g., Gardiner v. Walmart, Inc.*, No. 20-CV-04618-JSW, 2021 WL 4992539, at *5 (N.D. Cal. July 28, 2021) (dismissing for want of standing; “Plaintiff, however, never alleges that he read or relied on the Privacy Policy and offers no facts to support this conclusory allegation.”).

Plaintiffs, in short, failed to plead the plausible allegations that support an Article III injury. “[S]tanding is evaluated on an injury-by-injury basis[,]” *Flynn*, 2016 WL 5341749, at *3 (citing *Davis v. FEC*, 554 U.S. 724, 734 (2008)), and on a plaintiff by plaintiff basis. *Hochendoner v. Genzyme Corp.*, 823 F.3d 724, 733 (1st Cir. 2016) (“the plaintiff-by-plaintiff and claim-by-claim analysis required by standing doctrine demands allegations linking each plaintiff to each of these injuries”). Thus, Ticketmaster asks this Court to dismiss Plaintiffs’ claims, and, at a minimum, strike those theories on which the Court agrees the law negates standing.

2. Plaintiffs Fail to Allege Traceability

Plaintiffs’ standing problems don’t end with injury. They also fail on traceability because they fail to allege how their data at issue could be fairly traced

to any recoverable injuries. *See Greenstein v. Noblr Reciprocal Exch.*, No. 22-17023, 2024 WL 3886977, at *3 (9th Cir. Aug. 21, 2024) (affirming a district court’s finding that plaintiff failed to sufficiently plead causation element of Article III standing where the alleged injuries were not “fairly traceable” to the defendant); *Winsor v. Sequoia Benefits & Ins. Servs., LLC*, 62 F.4th 517, 525 (9th Cir. 2023) (same).

Plaintiffs cannot establish traceability because the Complaint does not establish any causal link between Plaintiffs’ claimed harms and the Data Incident. For starters, Plaintiffs Fitzgerald, Garcia-Nixon, and Neve fail to allege whether they received data breach notification letters such that Plaintiffs plead no reason to believe their data was at risk. (*See* Compl. ¶¶ 28–37, 51–54.) Indeed, similar data breach cases demonstrate that absent a notice from the defendant, Plaintiffs cannot identify the requisite underlying connection between their stated harms and the Data Incident. *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1036 (N.D. Cal. 2019) (where Bass did not allege he received a data breach notice, and the court found “the facts do not trace to the data breach at all or are so common the infinite possibilities forecloses plausibility.”) Thus, Plaintiffs Fitzgerald, Garcia-Nixon, and Neve fail to plead traceability, which is a complete bar to recovery.

Traceability is likewise wanting for the five Plaintiffs⁵³ who allegedly experienced fraudulent activity on their payment cards. Plaintiffs do not allege their CVV codes were included in the Data Incident, do not allege the hashed data was actually rendered usable, or do not explain how “credit card information such as the last four digits of their payment cards” leads to fraudulent charges on payment cards. (Compl. ¶ 473.) Thus, without more, “[t]here is simply no plausible explanation for how Plaintiffs’ alleged harm—like fraudulent charges—are linked in any way to the information, most of which is public information, involved in this data breach.” *In re Samsung Data Sec. Breach Litig.*, 761 F. Supp. 3d 781, 801 (D.N.J. Jan. 3, 2025).

Additionally fatal to their claims, Plaintiffs fail to state whether the allegedly fraudulent transactions were on a card that was ever used at Ticketmaster, that their specific card information was implicated in the Data Incident, or that the Data Incident was the only data breach they have suffered. Rather, they ask the Court to engage in an extreme leap of logic without any supporting allegations. Absent such allegations, no Plaintiff can meet their traceability pleading obligations. *Baysal v. Midvale Indemnity Co.* is instructive. 78 F.4th 976 (7th Cir. 2023). There, the Seventh Circuit found no standing where the plaintiffs failed to show how unauthorized charges and fraudulent accounts opened in their names could be traced to the disclosure of their driver’s license numbers. *Id.* at 978–80. Likewise,

⁵³ Including Plaintiffs Anderson, Fitzgerald, Garcia-Nixon, Lozoya, and Thomas.

Plaintiffs make no connection between the information involved in the Data Incident (unusable credit card information) to their alleged harm (fraudulent charges).

As further evidence of lack of traceability, all Plaintiffs fail to plead whether *any* of their data was exposed in the Data Incident. Instead, Plaintiffs blanketly describe the data they shared with Ticketmaster without stating whether any of that data was included in the Data Incident. (Compl. ¶¶ 23, 28, 33, 38, 43, 47, 51, 55, 60, 64 (stating Plaintiffs “provided Ticketmaster with at least [their] name, address, email, phone number, payment card information and transaction information”).) Plaintiffs also detail *potential* information exposed within the Data Incident for potentially impacted Ticketmaster customers without identifying which of their personal information was *actually* impacted by the Data Incident. (Compl. ¶¶ 202, 472–73.) These and other pleading failures warrant dismissal for lack of Article III standing. Alternatively, the Court should strike each injury for which Plaintiffs fail to plead traceability.

B. California Plaintiffs’ Claims Under the California Consumer Privacy Act Fail

The California Plaintiffs’ claims under the California Consumer Privacy Act (“CCPA”) fail as a matter of law for three independent reasons. *First*, the payment card information that the California Plaintiffs allege is at issue does not constitute “personal information” under the CCPA. *Second*, no named California Plaintiff alleges that their own passport numbers were involved in the Data Incident (or even

collected by Ticketmaster or Live Nation). ***Third***, the California Plaintiffs failed to comply with the CCPA's mandatory pre-suit notice requirement.

As such, the CCPA claim must be dismissed pursuant to Rule 12(b)(6) for failure to state a claim, and Rule 12(b)(1) for lack of subject matter jurisdiction.

1. The California Plaintiffs' CCPA Claim

The CCPA allows for a limited private right of action, stating that:

Any consumer whose nonencrypted and nonredacted personal information, as defined in [Section 1798.81.5(d)(1)(A) of the California Civil Code] . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action

Cal. Civ. Code § 1798.150(a)(1). "Personal Information," in turn, is defined in Section 1798.81.5(d)(1)(A), in relevant part, as:

An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted . . .

(ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

(iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

In their Complaint, the California Plaintiffs never allege that full credit card numbers with expiration dates and CVV codes—in other words the “credit card number” with the “required security code”—were stolen from Ticketmaster. Nowhere do the Plaintiffs allege that the CVV code, necessary for credit card transactions, was part of the Data Incident. Instead, they allege that certain incomplete debit and credit card information was involved, such as “the last four digits of [] payment cards and expiration dates.” (Compl. ¶ 473.)

Additionally, while the Complaint vaguely asserts that “passport numbers may have been impacted for some individuals,” (Compl. ¶ 411), including for “a certain number of Class Members,” (Compl. ¶ 561), the California Plaintiffs do not allege that their passport information was involved in the Data Incident.

2. California Plaintiffs Cannot Assert a Cognizable CCPA Claim

The Complaint fails to allege a cognizable CCPA claim because (a) the allegations regarding payment card information and passport numbers are insufficient as a matter of law, and (b) the California Plaintiffs lack standing to assert a CCPA claim for purported compromise of other, unknown individuals’ passport numbers.

i. *Incomplete Payment Card Data Without CVV Codes Are Not “Personal Information” for Purposes of CCPA’s Private Right of Action*

The California Plaintiffs’ allegations regarding payment card information are insufficient because such information does not constitute “personal information” under the CCPA.

Ticketmaster notified its potentially impacted customers about the Data Incident out of an abundance of caution. Ticketmaster later confirmed that the data, as Plaintiffs implicitly acknowledge, did not include full credit card numbers in plain text with associated CVV codes. (*See* Compl. ¶¶ 451, 455, 457, 472–73.) Therefore, Plaintiffs’ allegations regarding payment card information do not meet the definition of “personal information” for purposes of the CCPA’s private right of action (or, for that matter, under California’s data breach notification statute, Cal. Civ. Code § 1798.82(h)).

These allegations are a far cry from the definition of “personal information” under California law. *Gardiner v. Walmart Inc.*, No. 20-CV-04618-JSW, 2021 WL 2520103, at *3 (N.D. Cal. Mar. 5, 2021) (dismissing CCPA claim where the plaintiff “generally refer[red] to financial information and credit card fraud, [but did] not allege the disclosure of a credit or debit card or account number, and the required security or access code to access the account”). **First**, California Plaintiffs do not allege the impacted data includes a CVV code which is required under the CCPA;

and thus there is no “required security code, access code, or password that would permit access to an individual’s financial account” for any Plaintiff. *See* Cal. Civ. Code § 1798.81.5(d)(1)(A)(iii). ***Second***, to the extent Plaintiffs are relying on the “last four digits of card numbers,” these are not an “account number or credit or debit card number.” *Id.*

In addition, the Court need not accept Plaintiffs’ baseless allegations that there might be more data involved (*e.g.*, “Ticketmaster’s disclosure of the Data Breach has been insufficient,” (Compl. ¶ 561)), without some actual basis for the conclusory statement. *Twombly*, 550 U.S. at 570 (holding that a plaintiff cannot merely allege conduct that is conceivable but must instead allege “enough facts to state a claim to relief that is plausible on its face”).

ii. *The California Plaintiffs Fail to Plead that California Passport Numbers Were Included in the Data Incident*

The Complaint additionally fails to adequately plead that passport numbers pertaining to the California Plaintiffs or the California Ticketmaster Subclass were included in the Data Incident. Instead, the California Plaintiffs merely allege that some “passport information” (not “numbers”) for “certain California Subclass members” may have been provided to Ticketmaster or Live Nation (but not included in the Data Incident), and that “passport numbers may have been impacted for some individuals” more broadly. (Compl. ¶¶ 411, 565.) These allegations cannot form the basis of a CCPA claim.

First, simply saying that the data was given to Ticketmaster itself is not enough: to assert a claim under the CCPA, the “personal information” at issue must have been “subject to an unauthorized access and exfiltration, theft, or disclosure,” not simply *provided to* the defendant. Cal. Civ. Code § 1798.150(a)(1). These allegations thus fail to raise a plausible claim that passport numbers were potentially involved in the Data Incident. *See Iqbal*, 556 U.S. at 678 (holding in order to state a plausible claim, a complaint must plead “factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged”).

Second, to the extent Plaintiffs vaguely allege some other individuals’ passport numbers may have been involved in the Data Incident outside of the California Plaintiffs or the California Subclass, such individuals are not members of the putative class of California residents that California Plaintiffs seek to represent in connection with their CCPA claim, and categorically fall outside the ambit of the CCPA. *See, e.g., Sifuentes v. X Corp.*, No. 24-CV-00590-SK, 2024 WL 4953431, at *8 (N.D. Cal. Dec. 2, 2024) (“[T]he CCPA is clear that it does not apply to non-resident plaintiffs.”) (citing *Delgado v. Meta Platforms, Inc.*, 718 F. Supp. 3d 1146, 1154 (N.D. Cal. 2024)).

3. *California Plaintiffs Lack Standing to Assert a CCPA Claim*

The California Plaintiffs additionally lack standing to assert a CCPA claim regarding the passport numbers allegedly at issue. To establish standing, a plaintiff must allege, among other things, an “injury in fact”—something the California Plaintiffs have failed to (and cannot) allege generally, nor specifically as it relates to passport information. *See Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). To establish injury in fact, a plaintiff must show that he or she suffered “an invasion of a legally protected interest.”⁵⁴ *Lujan*, 504 U.S. at 560 (internal quotation marks omitted).

Here, the Complaint fails to allege that any named California Plaintiff’s passport number was involved in the Data Incident, and further fails to allege that Ticketmaster or Live Nation even collected it in the first place. Thus, the California Plaintiffs do not have standing to assert a CCPA claim solely based on the passport numbers of “other, unidentified members of the class to which they belong and which they purport to represent.” *Doe 1 v. GitHub, Inc.*, 672 F. Supp. 3d 837, 849 (N.D. Cal. 2023) (quoting *Warth v. Seldin*, 422 U.S. 490, 502 (1975)); *see also Lewis v. Casey*, 518 U.S. 343, 357 (1996).

⁵⁴ The invasion of the legally protected interest must additionally be “concrete and particularized” and “actual or imminent, not conjectural or hypothetical.” *Lujan*, 504 U.S. at 560.

For the foregoing reasons, the California Plaintiffs' CCPA claim should be dismissed.

C. Plaintiffs' Breach of Contract Claims Fail

Plaintiffs' breach of contract claims also fail. The five home states implicated by the Complaint—California, Massachusetts, Montana, New York, and Washington, D.C.—require similar elements to plead a breach of contract claim (and those elements will feel familiar to litigants in others states as well): (i) existence of a contract, (ii) plaintiff's performance, (iii) defendant's breach, and (iv) resulting damages to the plaintiff.⁵⁵ But Plaintiffs fail to identify any contractual provisions that were breached and fail to allege recoverable damages.

1. Plaintiffs Cannot Identify Any Breached Contractual Provisions

Each Plaintiff agreed to the Privacy Policy and the Terms of Use. The Privacy Policy specifically states what Ticketmaster will do to protect customers' information:

⁵⁵ *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 610 (9th Cir. 2020) (applying California law); *Lindstrom v. Polaris Inc.*, No. CV 23-137-BLG-SPW-TJC, 2024 WL 4237732, at *10 (D. Mont. Aug. 9, 2024), *report and recommendation adopted*, No. CV 23-137-BLG-SPW, 2024 WL 4275619 (D. Mont. Sept. 24, 2024) (citing *Kostelecky v. Peas in a Pod LLC*, 518 P.3d 840, 852 (Mont. 2022) (applying Montana law)); *Ebomwonyi v. Sea Shipping Line*, 473 F. Supp. 3d 338, 347 (S.D.N.Y. 2020), *aff'd*, No. 20-3344, 2022 WL 274507 (2d Cir. Jan. 31, 2022) (applying New York law); *Barros v. Gov't Emps. Ins. Co., Inc.*, 79 F. Supp. 3d 32, 36 (D.D.C. 2015) (applying D.C. law); *Squeri v. Mount Ida Coll.*, 954 F.3d 56, 71 (1st Cir. 2020) (applying Massachusetts law).

We have security measures in place to protect your information. The security measures we use will depend on the type of information collected.⁵⁶

Ticketmaster did just that. As Plaintiffs concede, all the payment card information stored by Ticketmaster in the Snowflake Environment was hashed or only included the last 4 digits, (Compl. ¶¶ 457, 472, 473), and Plaintiffs do not allege that any CVV codes were impacted by the Data Incident, rendering the cards unusable. In addition, Ticketmaster’s vendor, Snowflake, committed to protecting the information entrusted to it, holding numerous security certifications regarding how they protected the information.⁵⁷

Thus, Ticketmaster implemented “security measures to protect [Plaintiffs’] information” as required by its Privacy Policy. Ignoring this fact, Plaintiffs look to non-contractual Ticketmaster webpages, (Compl. ¶ 406), and general statements within the Privacy Policy such as “handling your personal information with respect,” (Compl. ¶ 403), to manufacture alleged contractual obligations. That effort fails.

Courts have even dismissed cases where there are general statements about keeping information “safe,” not merely treating it with “respect” as Plaintiffs point

⁵⁶ Privacy Policy, *supra* note 9 at “Looking After Your Information.”

⁵⁷ Compl. ¶ 270; Whitner Decl. ¶ 4, Ex. 3; *Snowflake Security Hub*, Snowflake, <https://www.snowflake.com/en/why-snowflake/snowflake-security-hub/> (last visited June 16, 2025) (“Snowflake services and accounts are designed for security, lowering the risk of vulnerabilities and breaches with features that help customers configure comprehensive levels of security for their data and users.”).

to here. For example, in *Zappos*, the court “dismis[s]e[d] the contractual claims,” where, the plaintiffs “allege[d] that Zappos breached a contract to safeguard their data[.]” and pointed to “statements on Zappos’s website indicat[ing] that its servers were protected by a secure firewall and that customers’ data was safe.” *In re Zappos.com, Inc.*, No. 3:12-CV-00325-RCJ, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013). The court held unequivocally that these statements “do not create any contractual obligations[.]” *Id.*; see also *Beverage Distribs., Inc. v. Olympia Brewing Co.*, 440 F.2d 21, 29 (9th Cir. 1971) (“A gratuitous and unsolicited statement of policy or of intention which receives the concurrence of the party to whom it is addressed, does not constitute a contract.”). *Smahaj v. Retrieval-Masters Creditors Bureau, Inc.*, 131 N.Y.S.3d 817, 826 (N.Y. Sup. Ct. 2020) (dismissing a data breach contract claim where the plaintiff failed to identify the provision of the purported contract that required the defendant to safeguard plaintiff’s information on a third party’s network and noting that the defendant’s privacy notice did not indicate that the defendant would safeguard data on a third party’s network); *Wallace v. Health Quest Sys., Inc.*, No. 20-CV-545, 2021 WL 1109727, at *10 (S.D.N.Y. Mar. 23, 2021) (dismissing express breach of contract claim where privacy policy did not commit defendant to prevent a data breach).

Perhaps acknowledging that their website snippets cannot actually be incorporated into the contract they claim was breached, Plaintiffs also try to invoke

Ticketmaster’s Privacy Policy. But Plaintiffs never identify the specific provisions that allegedly were breached. For example, Plaintiffs accuse Ticketmaster of breaching the *Privacy Policy*⁵⁸ (a contract) and *Commitments*⁵⁹ (not a contract) by failing to: (i) enable MFA for its Snowflake accounts; (ii) rotate or disable the credentials of old Snowflake accounts; and (iii) implement “network allow lists,” which, according to Plaintiffs, could have restricted Snowflake account access to certain locations or trusted Users. (Compl. ¶¶ 456, 520.) These claimed “breaches,” however, amount to nothing more than a data security wishlist. Neither the Privacy Policy nor the Commitments (even if they contained contractual provisions, which they do not) expressly state Ticketmaster would perform any of Plaintiffs’ cited methods of data security.

To the contrary, Plaintiffs agreed in all caps in their Terms of Use: “[TICKETMASTER DOES] NOT GUARANTEE THAT THE SITE WILL ALWAYS BE SAFE, SECURE, OR ERROR-FREE, OR THAT THE SITE WILL ALWAYS FUNCTION WITHOUT DISRUPTIONS, DELAYS, OR

⁵⁸ The Privacy Policy is incorporated by reference into the Parties’ governing contractual agreement—the Terms of Use. *See also* Privacy Policy, *supra* note 9.

⁵⁹ The Commitments are not incorporated by reference into the Terms of Use. Instead, the “Commitments” are located on an archived webpage on Ticketmaster’s website: Ticketmaster, *Our Commitments*, <https://web.archive.org/web/20230517182539/https://privacy.ticketmaster.com/our-commitments> (archived May 17, 2023) (“Privacy Commitments”).

IMPERFECTIONS.”⁶⁰ The Privacy Policy also sets the standard for what data protections will be in place:

We have security measures in place to protect your information. The security measures we use will depend on the type of information collected.⁶¹

In other words, Plaintiffs were not promised that data breaches like this one would not occur; they were actually (and prudently) told that Ticketmaster would implement security measures to protect the data, without promising that there would never be a breach, to which they agreed.

Other courts have enforced admonitory language just like Ticketmaster’s and dismissed a whole range of causes of action. *See, e.g., In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 968 (S.D. Cal. 2012) (“Thus, in the presence of clear admonitory language that Sony’s security was not ‘perfect,’ no reasonable consumer could have been deceived.”); *see also Baton v. Ledger SAS*, 740 F. Supp. 3d 847, 902 (N.D. Cal. 2024) (“Likewise, here, Ledger disclosed that any information inputted on the Internet is ‘not fully secure.’ Thus, consumers could not have been misled into thinking that providing Ledger with their PII online would be fully secure.”).

⁶⁰ Terms of Use § 14, *supra* note 8.

⁶¹ Privacy Policy, *supra* note 9 at “Looking After Your Information.”

In every breach of contract case, the alleged breach must be tied to the express contractual promises—Plaintiffs fail to meet that pleading burden here. *Miron v. Herbalife Int’l, Inc.*, 11 F. App’x 927, 929 (9th Cir. 2001) (finding “[i]n order for a breach of contract action to be based on an instrument in writing, the writing must express the obligation sued upon” (cleaned up) (citations omitted)).

2. *Plaintiffs’ Damages Are Not Recoverable by Contract*

Beyond the failure to identify an actionable breach, Plaintiffs also fail to plead recoverable damages. Ticketmaster has already discussed Plaintiffs’ failure to plead injury (*see supra* Section V.A.). Rather than repeat that argument, Ticketmaster notes that courts often simply apply the lack of standing analysis to the lack of damages analysis one-to-one. *Weaver v. Aetna Life Ins. Co.*, No. 308-CV-00037-LRH-VPC, 2008 WL 4833035, at *4 (D. Nev. Nov. 4, 2008) (dismissing a substantive cause of action for lack of damages for the same reasons discussed in the court’s Article III injury analysis), *aff’d*, 370 F. App’x 822 (9th Cir. 2010).

But there is an additional reason to dismiss the contract claim. Plaintiffs’ claimed damages are not recoverable under the express, enforceable limitation of liability contractual provision to which they agreed.⁶²

⁶² Ticketmaster notes that there may be a divergence under Montana law on limitation clauses. *See, e.g.*, Mont. Code Ann. § 28-2-702. Thus, at this time, Ticketmaster makes this argument only as to Plaintiffs Anderson, Fitzgerald, Garcia-Nixon, Lozoya, Neve, O’Hara, Thomas, and Xian.

IN NO EVENT WILL WE . . . BE RESPONSIBLE OR LIABLE TO YOU OR ANYONE ELSE FOR, AND YOU HEREBY KNOWINGLY AND EXPRESSLY WAIVE ALL RIGHTS TO SEEK, DIRECT, INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OF ANY TYPE . . . YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT WE WILL HAVE NO LIABILITY OR RESPONSIBILITY WHATSOEVER FOR . . . (c) ANY UNAUTHORIZED ACCESS TO OR USE OF OUR SECURE SERVERS AND/OR ANY AND ALL PERSONAL INFORMATION AND/OR FINANCIAL INFORMATION STORED THEREIN.⁶³

Limitation of liability provisions are enforced in each home state for Plaintiffs Anderson, Fitzgerald, Garcia-Nixon, Lozoya, Neve, O'Hara, Thomas, and Xian.⁶⁴ Courts like the one in *Bass v. Facebook, Inc.*, 394 F. Supp. 3d at 1037–38, have enforced clauses just like this one:

[O]ur liability shall be limited to the fullest extent permitted by applicable law, and under no circumstance will we be liable to you for any lost profits, revenues, information, or data, or consequential, special, indirect, exemplary, punitive, or incidental damages.

Thus, Plaintiffs' breach of contract claim is barred by express limitation of liability.

⁶³ Terms of Use § 15, *supra* note 8.

⁶⁴ *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1037–38 (N.D. Cal. 2019); *Indem. Ins. Co. of N. Am. v. Expeditors Int'l of Wash., Inc.*, 533 F. Supp. 3d 158, 163 (S.D.N.Y. 2021); *Brown v. 1301 K St. Ltd. P'ship*, 31 A.3d 902, 907–08 (D.C. 2011); *Kemper Ins. Cos., Inc. v. Fed. Exp. Corp.*, 115 F. Supp. 2d 116, 122 (D. Mass. 2000), *aff'd*, 252 F.3d 509 (1st Cir. 2001).

3. *Plaintiffs’ Breach of Implied Contract Claims Also Fail*

Tucked into their generically labeled “breach of contract” claim, Plaintiffs suggest they *also* are alleging breach of an implied contract. (Compl. ¶ 502.) But there can be no implied breach of contract where there is an express contract addressing the same subject matter between the parties. *See Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1078, 1094–95 (N.D. Cal. 2022) (applying California law);⁶⁵ *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 717–18 (8th Cir. 2017).

In *Hammerling v. Google LLC*, plaintiffs accused Google of collecting “sensitive personal data” from Android smartphones without plaintiffs’ knowledge or consent, and alleged plaintiffs had an implied contract with Google prohibiting collection of this sensitive information. 615 F. Supp. 3d at 1078, 1095. The court dismissed plaintiff’s implied contract claim because an express contract between the parties governed the same subject matter—the scope and purpose of data protection. *Id.* at 1096. Similarly, in *Krefting v. Kaye-Smith Enters. Inc.*, No. 2:23-CV-220, 2023 WL 4846850, at *6 (W.D. Wash. July 28, 2023), a data breach case, the court

⁶⁵ *See also Sullivan v. O’Connor*, 961 N.E.2d 143, 153 (Mass. App. Ct. 2012) (applying Massachusetts law); *McNulty v. Bewley Corp.*, 596 P.2d 474, 476 (Mont. 1979) (applying Montana law); *SAA-A, Inc. v. Morgan Stanley Dean Witter & Co.*, 721 N.Y.S.2d 640, 242 (App. Div. 2001) (applying New York law); *Albrecht v. Comm. on Emp. Benefits of the Fed. Reserve Emp. Benefits Sys.*, 357 F.3d 62, 69 (D.C. Cir. 2004) (applying D.C. law).

held the existence of defendant’s valid Agreement prohibited plaintiff’s implied contract claim. *Id.* at *7.

So too here. Plaintiffs acknowledge they have agreed to the Terms (an express contract) and that the Terms incorporate the Privacy Policy. (Compl. ¶¶ 400–09, 498.) With the Terms already addressing data protection, no implied contract claim will lie (if it is in fact even alleged).

i. *There Is No Implied Duty to Protect Plaintiff’s Data*

Plaintiffs impermissibly assume, without pleading factual support, that because Ticketmaster collected Plaintiffs’ data and subsequently suffered the Data Incident by a third-party criminal, Ticketmaster breached a duty to protect Plaintiffs’ information. Courts have rejected such insufficient pleading as a matter of law, dismissing similar claims for breach of implied contract.⁶⁶ In *Kuhns*, the Eighth Circuit upheld dismissal of both breach of contract and breach of implied contract claims because that plaintiff did not allege that the defendant “affirmatively promised that its customer data would not be hacked, and such a promise may not

⁶⁶ See, e.g., *Kuhns*, 868 F.3d at 717–18 (“The implied premise that because data was hacked [a defendant’s] protections must have been inadequate is a ‘naked assertion[] devoid of further factual enhancement’ that cannot survive a motion to dismiss.” (quoting *Iqbal*, 556 U.S. at 678)); *Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 51–52 (D. Ariz. 2021) (rejecting premise that “[b]ecause there was a data breach, [defendant’s] data security must have been inadequate, which is a breach of the implied contracts”).

be plausibly implied.” *Id.* at 717. Likewise, Ticketmaster never affirmatively promised cybercriminals would not steal Plaintiffs’ data, and any such promise may not be implied. Because Plaintiffs rely on the same broken logic rejected in *Kuhns*—imposing a contractual duty never assented to by the defendant—their claims should be dismissed.

D. Plaintiffs’ Negligence Claims Fail

Plaintiffs’ acknowledgment of the Terms and Privacy Policy, together with Ticketmaster’s storing of unusable payment card data without the CVV code in the Snowflake Environment does not just negate Plaintiffs’ purported implied contract claims. For most Plaintiffs, the Terms also require dismissal of their negligence claims based on the economic loss doctrine.⁶⁷ And all Plaintiffs fail to plead quintessential elements of their negligence claims: causation and damages.⁶⁸

⁶⁷ As noted above, Montana law is less clear on the economic loss doctrine in the services space, though it has addressed it in the strict liability/products case. *See Thompson v. Neb. Mobile Homes Corp.*, 647 P.2d 334, 337 (Mont. 1982). Thus, at this time, Ticketmaster is making this argument only as to Plaintiffs Anderson, Fitzgerald, Garcia-Nixon, Lozoya, Neve, O’Hara, Thomas, and Xian but not Plaintiffs Madden and Murphy.

⁶⁸ *See, e.g., Papageorge v. Zucker*, 169 A.3d 861, 863 (D.C. 2017) (“To prevail on a claim of negligence, a plaintiff must show that the defendant owed him a duty of care, that the defendant breached the duty, and that the plaintiff suffered damages as a result.”); *Berkley v. Dowds*, 152 Cal. App. 4th 518, 526-28 (2007) (same applying California law); *Sikorski v. Johnson*, 143 P.3d 161, 164 (Mont. 2006) (same applying Montana law); *Kraut v. City of New York*, 925 N.Y.S.2d 624, 626 (App. Div. 2011) (same applying New York law); *Leavitt v. Brockton Hosp., Inc.*, 907 N.E.2d 213, 215–16 (Mass. 2009) (same applying Massachusetts law).

1. The Negligence Claims Are Barred by the Economic Loss Doctrine

As a general matter, the economic loss doctrine precludes recovery in tort for alleged negligence on a topic covered by a contract unless the plaintiff can demonstrate physical injury or property damage—in other words, non-economic losses. *Sheen v. Wells Fargo Bank, N.A.*, 505 P.3d 625, 632 (Cal. 2022).⁶⁹ Data breach jurisprudence states “‘claims for monetary losses between contractual parties are barred by the economic loss rule . . . when they arise from — or are not independent of — the parties’ underlying contracts.’” *Terpin v. A.T. & T Mobility LLC*, 118 F.4th 1102, 1114 (9th Cir. 2024) (quoting *Sheen*, 505 P.3d at 625).

Plaintiffs fall squarely within this rule. They acknowledge a contractual relationship. (Compl. ¶¶ 497–512.) While incorrect, they accuse Ticketmaster of breaching the same duties Plaintiffs derive from the contract. (*Compare* Compl. ¶¶ 578–89 *with id.* at ¶¶ 497–512.) They plead only economic losses. (Compl. ¶¶ 587, 589.) Thus, their negligence claim fails as a matter of law.

⁶⁹ See also *Aguilar v. RP MRP Wash. Harbour, LLC*, 98 A.3d 979, 985–86 (D.C. 2014) (“The economic loss doctrine in the District of Columbia bars recovery of purely economic losses in negligence[.]”); *Cumis Ins. Soc’y, Inc. v. BJ’s Wholesale Club, Inc.*, 918 N.E.2d 36, 46 (Mass. 2009) (“[T]he economic loss doctrine bars recovery unless the plaintiffs can establish that the injuries they suffered due to the defendants’ negligence involved physical harm or property damage, and not solely economic loss.”); *D’Ambrosio v. Engel*, 741 N.Y.S.2d 42, 44 (App. Div. 2002) (“A defendant ‘may be liable in tort when it has breached a duty of reasonable care distinct from its contractual obligations.’”) (citation omitted).

Plaintiffs’ allegations that the Data Incident caused emotional harm does not help them. (*See* Compl. ¶¶ 26, 31, 36, 41, 45, 49, 53, 57, 62 (claiming “emotional distress and anxiety resulting from the theft of [their] Personal Information and responding to identity theft”).) A plea to emotional distress (real or otherwise) does not save a negligence claim from the economic loss doctrine. For example, in *Pearl v. Coinbase Global, Inc.*, No. 22-CV-03561, 2024 WL 3416505, at *6 (N.D. Cal. July 15, 2024), the court rejected plaintiffs’ argument that their emotional damages including stress, anxiety, and outrage constitute physical injury that can circumvent the economic loss doctrine.⁷⁰ And generically pled emotional damages likewise fail because “conclusory allegations devoid of factual support . . . are not enough to support a claim for non-economic damages.” *Ramos v. Wells Fargo Bank, N.A.*, No. 23-CV-0757, 2023 WL 5310540, at *3 (S.D. Cal. Aug. 17, 2023).

The economic loss doctrine bars Plaintiffs’ negligence claims.

⁷⁰ *See Pegasus Trucking, LLC v. Asset Redeployment Grp., Inc.*, No. 19-CV-10339, 2021 WL 1234879, at *7 (C.D. Cal. Feb. 16, 2021) (applying California law and holding that the plaintiffs’ claim of emotional distress in connection with a fraud claim, which was supported by only “conclusory statements,” was “insufficient to allege noneconomic loss” and further noting that the plaintiffs cited “no authority for the proposition that there is an ‘emotional distress’ exception to the economic loss rule”); *In re Residential Capital, LLC*, 529 B.R. 806, 819 (Bankr. S.D.N.Y. 2015) (applying Massachusetts law and noting that emotional damages must manifest themselves physically to avoid the economic loss doctrine).

2. *Plaintiffs Cannot Prove Causation*

Plaintiffs also cannot prove that the Data Incident caused any of their alleged injuries. Ticketmaster protected the payment card data in the Snowflake Environment, including by not storing the CVV code with that data. The rest of the information accessed—such as name, contact information, and addresses—is publicly available. In the face of this, Plaintiffs have not pleaded any facts to plausibly allege how the Data Incident *caused* any of the damages they seek. Ticketmaster addressed this point in its Article III discussion above. *Lowy v. Daniel Def., LLC*, No. 1:23-CV-1338, 2024 WL 3521508, at *4 (E.D. Va. July 24, 2024) (finding “the complaint’s deficiencies under Article III also doom plaintiffs’ allegations of proximate cause”).

While Plaintiffs plead the legal conclusion of causation, they do not plead the plausible facts supporting the conclusion. (Compl. ¶ 589.) Such insufficient pleading warrants dismissal. *See, e.g., Holmes v. SIPC*, 503 U.S. 258, 268 (1992) (finding proximate cause “demand[s] . . . some direct relation between the injury asserted and the injurious conduct alleged.”); *Bass*, 394 F. Supp. 3d at 1036 (finding “[w]hat forecloses plaintiff Bass from establishing [causation] here is that none of the circumstantial evidence he provides plausibly connects to the data breach. Either the facts do not trace to the data breach at all or are so common the infinite possibilities forecloses plausibility.”)

Take, for example, the credit cards Plaintiffs claim were compromised. Plaintiffs do not allege *their* cards were impacted by the Data Incident. (Compl. ¶¶ 24, 29, 34, 39, 65.) They concede the cards that were impacted were unusable, and they do not allege the CVV codes were impacted. (Compl. ¶¶ 23, 28, 33, 38, 202, 457, 472.) Thus, Plaintiffs have failed to plead the necessary facts to prove causation.

3. Plaintiffs Cannot Prove Damages

Discussed *supra* at Section V.A., Plaintiffs' damages are not recoverable as a matter of law. The insufficiency of Plaintiffs' damages allegations is apparent in both the Article III injury-in-fact context and Plaintiffs' substantive negligence claim. *See Weaver*, 2008 WL 4833035, at *4 (dismissing plaintiff's negligence claim for lack of damages based on the same reasons addressed in the court's Article III analysis).

Plaintiffs Murphy and Madden's claimed damages are also unrecoverable because Montana law requires physical harm, and they make no physical harm allegations. *Maryland Cas. Co. v. Asbestos Claims Ct.*, 460 P.3d 882, 895–98 (Mont. 2020) (quoting Restatement (Second) of Torts §§ 315, 323, 324A); (Compl. ¶¶ 43–50); *see Quinalty v. FocusIT LLC*, No. CV-23-00207-PHX-JJT, 2024 WL 342454, at *1, *4 (D. Ariz. Jan. 30, 2024) (data breach case finding emotional

distress and lost time and money are not physical harm and dismissing the plaintiffs' negligence claim absent physical harm).

E. Montana Plaintiffs' MCPA Claim Fails

Montana Plaintiffs' claim under the Montana Unfair Trade Practices & Consumer Protection Act ("MCPA") should be dismissed because (i) they have not pleaded any unfair or deceptive act, nor (ii) have they shown reliance on any alleged deception.

To state a claim under the MCPA, the Montana Plaintiffs must allege: (1) they were consumers, as defined by the MCPA; (2) that Ticketmaster "use[d] or employ[ed]' an 'unfair or deceptive act[] or practice[] in the conduct of any trade or commerce'"; (3) causation; and (4) ascertainable loss. *Kostelecky*, 518 P.3d at 861.

First, the Montana Plaintiffs have not alleged Ticketmaster used or employed an unfair or deceptive practice because Plaintiffs have failed to identify a practice that is immoral, unethical, or substantially injurious, as required under Montana law. *See Rohrer v. Knduson*, 203 P.3d 759, 764 (Mont. 2009) ("[A]n unfair act or practice is one which offends established public policy and which is either immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers."). Indeed, "product superiority claims that are vague or highly subjective often amount to non[-]actionable puffery, [whereas] misdescriptions of specific or absolute characteristics of a product are actionable." *Southland Sod Farms v. Stover Seed*

Co., 108 F.3d 1134, 1145 (9th Cir. 1997) (internal quotation and citation omitted). While Plaintiffs allege Ticketmaster deceived consumers by misrepresenting the adequacy of Plaintiffs’ data security, (Compl. ¶¶ 400–07)—as discussed *supra*—Plaintiffs impermissibly rely upon vague and highly subjective statements about data security. (*See, e.g.*, Compl. ¶ 403 (citing the Privacy Policy provision which reads, “Our goal is to maintain your trust and confidence by handling your personal information with respect and putting you in control” rather than the actual section on data security).)

None of Plaintiffs’ allegations rise to the level of an act or practice that is “immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers.” *Rohrer*, 203 P.3d at 764. The Montana Supreme Court explains an “unfair . . . act” is substantially injurious to consumers when a party states “that a transaction involves rights, remedies or obligations that it does not involve.” *Anderson v. ReconTrust Co., N.A.*, 407 P.3d 692, 700 (Mont. 2017) (citing Admin. R. M. 23.19.101(1)(l) and finding those plaintiffs did not state an MCPA claim where they failed to allege that the defendant “misrepresent[ed] that the transaction ‘involve[d] rights, remedies or obligations that it d[id] not involve.’”)). But Ticketmaster did no such thing. In fact, Ticketmaster only promised that it had security measures in place, which it did. Plaintiffs concede that the credit card information at issue was hashed, and they do not allege the CVV codes associated

with the credit card was discoverable to the threat actors, which is consistent with Ticketmaster’s commitment in its Privacy Policy that the “security measures we use will depend on the type of information collected.”⁷¹ (Compl. ¶¶ 457, 472.)

Second, the Montana Plaintiffs fail to allege causation because Plaintiffs have not shown that they relied on any false statements to their detriment. *See Anderson*, 407 P.3d at 700 (“[T]he amended complaint was devoid of any factual assertion that, but for their reliance on [the defendant’s] initial alleged misrepresentation regarding their loan modification eligibility, [the plaintiffs] would have” not been harmed.). The Montana Plaintiffs state—in vague and conclusory fashion— “[h]ad [they] known that Ticketmaster would not adequately protect and instead release [their] Personal Information, [they] would either have sought to purchase tickets elsewhere or avoided purchasing tickets altogether.” (Compl. ¶¶ 46, 50.) But wholly missing from the Montana Plaintiffs’ allegations is any affirmative statement that they actually read the allegedly misleading statements, making it impossible for Plaintiffs to have relied upon these statements. *See Est. of Petersen v. Koelsch Senior Cmtys., LLC*, No. CV 22-11-BLG-SPW-TJC, 2025 WL 953709, at *14 (D. Mont. Feb. 21, 2025) (finding no causation under the MCPA where “there [was] no evidence Plaintiffs were even aware of the representations or relied upon them to their

⁷¹ Privacy Policy, *supra* note 9 at “Looking After Your Information.”

financial detriment”), *report and recommendation adopted*, No. CV 22-11-BLG-SPW, 2025 WL 914401 (D. Mont. Mar. 26, 2025).

In the absence of both an identifiable unfair act or practice and causation, the Montana Plaintiffs’ MCPA claims fail to show “that the pleader is entitled to relief,” as required under Fed. R. Civ. P. 8. And because Plaintiffs fall short of Rule 8, they completely abandon Rule 9(b), failing to plead any of the MCPA allegations with particularity. *See, e.g., Guthridge v. Johnson & Johnson Corp.*, No. 22-CV-145-BLG-SPW-TJC, 2023 WL 6626175, at *3–5 (D. Mont. Sept. 22, 2023) (“demand[ing] that the circumstances constituting the alleged fraud ‘be specific enough to give defendants notice of the particular misconduct . . . so that they can defend against the charge and not just deny that they have done anything wrong’”) (quotation marks and citations omitted), *report and recommendation adopted*, No. CV 22-145-BLG-SPW, 2023 WL 6626163 (D. Mont. Oct. 11, 2023).

F. California Plaintiffs’ Unfair Competition Law Claim Fails

Plaintiffs assert a California statutory consumer protection claim under California’s Unfair Competition Law (“UCL”) on behalf of Plaintiffs and the Ticketmaster class, or alternatively on behalf of California named Plaintiffs and the California Ticketmaster Subclass. Plaintiffs’ UCL claim fails because they cannot show that they lack adequate legal remedies or any predicate “unlawful,” “fraudulent,” or “unfair” conduct. *See* CAL. BUS. & PROF. CODE § 17200.

California’s UCL is an equitable law allowing only equitable remedies (an injunction or restitution) if proven. A hallmark of equitable law is a pleading (based on plausible facts) that legal remedies are inadequate. Thus, the Ninth Circuit has affirmed the dismissal of UCL claims where the plaintiff “fail[ed] to demonstrate that she lacks an adequate legal remedy.” *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 845 (9th Cir. 2020).

Numerous courts have dismissed UCL claims at the motion to dismiss stage in the wake of *Sonner* for failure to show lack of adequate remedies. *See, e.g., In re Macbook Keyboard Litig.*, No. 5:18-cv-02813-EJD, 2020 WL 6047253, at *4 (N.D. Cal. Oct. 13, 2020); *Gibson v. Jaguar Land Rover N. Am., LLC*, No. CV 20-00769-CJC (GJSx), 2020 WL 5492990, at *3 (C.D. Cal. Sept. 9, 2020); *Schertz v. Ford Motor Co.*, No. CV 20-03221-TJH (PVCx), 2020 WL 5919731, at *2 (C.D. Cal. July 27, 2020); *Adams v. Cole Haan, LLC*, No. SACV 20-913 JVS (DFMx), 2020 WL 5648605, at *2 (C.D. Cal. Sept. 3, 2020) (“The clear rule in *Sonner* [is] that plaintiffs must plead the inadequacy of legal remedies before requesting equitable relief[.]”).

As the Court in *In re Apple Processor Litig.* recently explained, where a plaintiff grounds his UCL claims in the same facts as his legal claims, he necessarily concedes adequacy of the possible legal remedies and thus he has not pleaded what the UCL requires. No. 22-16164, 2023 WL 5950622, at *2 (9th Cir. Sept. 13, 2023); *see also Webb v. Rejoice Delivers LLC*, No. 22-CV-07221-BLF, 2025 WL 974996,

at *4 (N.D. Cal. Apr. 1, 2025) (“Because Plaintiff’s UCL claim is predicated on the identical wage and hour violations alleged in Plaintiff’s first through eighth claims, Plaintiff has not and cannot allege that his legal remedies are inadequate.”). And the Ninth Circuit affirmed dismissal in *In re Apple Processor Litig.* in *Sonner*’s wake. *In re Apple Processor Litig.*, 2023 WL 5950622, at *2 (“[p]laintiffs were obligated to allege that they had no adequate legal remedy in order to state a claim for equitable relief” and failed to do so).

Here, Plaintiffs use the UCL as a vehicle to reallege their other claims (*see, e.g.,* Compl. ¶¶ 497–534, 559–589)—which as the *Webb* Court noted, sinks the UCL claim under *Sonner*. *See Webb*, 2025 WL 974996, at *4. Therefore, Plaintiffs’ failure to elicit an inadequate legal remedy warrants dismissal.

Even beyond a *Sonner* bar, Plaintiffs’ allegations fail under Federal Rule of Civil Procedure 9(b). Plaintiffs plead in conclusory fashion that Ticketmaster made “representations and omissions” and that such representations and omissions were “fraudulent” within the meaning of the UCL. (*See, e.g.,* Compl. ¶ 548.) But Rule 9(b) requires more. Plaintiffs were required “to ‘state with particularity the circumstances constituting fraud or mistake,’ including ‘the who, what, when, where, and how of the misconduct charged’” as well as “‘what is false or misleading about a statement, and why it is false.’” *Ebeid ex rel. U.S. v. Lungwitz*, 616 F.3d 993, 998 (9th Cir. 2010) (quoting *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097,

1106 (9th Cir. 2003)). And each Plaintiff must plead reliance with particularity. *See, e.g., Diep v. Apple, Inc.*, No. 22-16514, 2024 WL 1299995, at *3 (9th Cir. Mar. 27, 2024) (in Rule 9(b) analysis; “[a]lthough Plaintiffs do identify a number of Apple’s statements they allege to be ‘misleading,’ they do not explain why those statements would be misleading to a reasonable consumer, whether and how those statements induced reliance, or why reliance was reasonable”).

The same standards apply to statements of nondisclosure: “[because] nondisclosure is a claim for misrepresentation in a cause of action for fraud, it (as any other fraud claim) must be pleaded with particularity under Rule 9(b).” *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1127 (9th Cir. 2009).⁷²

Here, while Plaintiffs’ Complaint cites to selected statements, there is no allegation of when each Plaintiff saw a statement, how, and whether each Plaintiff in fact relied on it. Because the Complaint fails to tie any Ticketmaster statements

⁷² *See Krystofiak v. BellRing Brands, Inc.*, 737 F. Supp. 3d 782, 802 (N.D. Cal. 2024) (citing *Hodsdon v. Mars, Inc.*, 891 F.3d 857, 861 (9th Cir. 2018)) (With respect to a claim based on an alleged *omission* (as appears to be the case here), the Ninth Circuit requires that “either the omission be (i) contrary to an actual representation or (ii) of a fact for which the defendant had a duty to disclose.”); *Castillo v. Prime Hydration LLC*, 748 F. Supp. 3d 757, 772 (N.D. Cal. 2024) (“To establish a duty to disclose under California law, a plaintiff must plead that (1) the defendant is in a fiduciary relationship with the plaintiff, (2) the defendant ha[s] exclusive knowledge of material facts not known to the plaintiff, (3) the defendant actively conceals a material fact from the plaintiff, or (4) the defendant makes partial representations but also suppresses some material fact.”) (quotation marks and citation omitted).

to Plaintiffs and then fails to tie these statements to any allegations of detrimental reliance, no claim is stated. Thus, because of both *Sonner* and Rule 9, Plaintiffs' UCL claims should be dismissed.

G. Plaintiffs Fail to State A Claim Under GBL § 349

Plaintiffs Anderson and Fitzgerald's New York's General Business Law § 349 allegations also fail. Section 349(a) states "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful." To plead a violation of Section 349, Plaintiffs must plead actual injury. *Koenigsberg v. Bd. of Trs. of Columbia Univ.*, No. 23 CIV. 1044 (PGG), 2024 WL 1256270, at *9 (S.D.N.Y. Mar. 22, 2024). Plaintiffs' Section 349 claim fails because they have not identified any deceptive acts or practices, *see supra* at Section V.E., and they fail to plead actual injury, *see supra* Section V.A. *See Koenigsberg*, 2024 WL 1256270, at *9 (finding plaintiffs must "allege that, on account of a materially misleading practice, [they] purchased a product and did not receive the full value of [their] purchase") (citation omitted).

VI. CONCLUSION

For the foregoing reasons, Ticketmaster respectfully requests dismissal of Consumer Plaintiff's Complaint, in its entirety, pursuant to Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure or, alternatively, move to strike portions of the Complaint pursuant to Rule 12(f).

DATED this 18th day of June, 2025.

GARLINGTON, LOHN & ROBINSON, PLLP

/s/ Emma L. Mediak

Emma L. Mediak
Leah T. Handelman
Elijah L. Inabnit
350 Ryman Street • P. O. Box 7909
Missoula, MT 59807-7909
Phone (406) 523-2500
Fax (406) 523-2595
elmediak@garlington.com
lthandelman@garlington.com
elinabnit@garlington.com

PAUL HASTINGS LLP

/s/ William K. Whitner

William K. Whitner (admitted *pro hac vice*)
Eric D. Stolze (admitted *pro hac vice*)
1170 Peachtree Street, N.E., Suite 100
Atlanta, GA 30309
T: 404.815.2228
F: 404.685.5228
kwhitner@paulhastings.com
ericstole@paulhastings.com

Manuel G. Berrelez (admitted *pro hac vice*)
2001 Ross Ave # 2700
Dallas, TX 75201
T: 972.936.7478
F: 972.936.7378
manuelberrelez@paulhastings.com

D. Scott Carlton (admitted *pro hac vice*)
515 South Flower Street
Twenty-Fifth Floor

Los Angeles, CA 90071
T: 213.683.6113
F: 213.996.3113
scottcarlton@paulhastings.com

James Pearl (admitted *pro hac vice*)
1999 Avenue of the Stars
27th Floor
Los Angeles, CA 90067
T: 310.620.5730
F: 310.620.5830
jamespearl@paulhastings.com

Sean Unger (*pro hac vice* forthcoming)
101 California Street
Forty-Eighth Floor
San Francisco, CA 94111
T: 415.856.7056
F: 415.856.7156
seanunger@paulhastings.com

Attorneys for Defendants TICKETMASTER
L.L.C. and LIVE NATION ENTERTAINMENT,
INC.

CERTIFICATE OF COMPLIANCE

Pursuant to L.R. 7.1(d)(2)(E) and the word count extension granted by Hon. Morris at the hearing held on May 22, 2025, I certify that this **Memorandum In Support of Ticketmaster’s Motion to Dismiss or, Alternatively, Motion to Strike the Consumer Plaintiffs’ Third Amended Representative Class Action Complaint** is printed with proportionately spaced Times New Roman text typeface of 14 points; is double-spaced; and the word count, calculated by Microsoft Office 365, is 15,401 words long, excluding Caption, Certificate of Service and Certificate of Compliance.

/s/ Emma L. Mediak
Attorney for Defendants TICKETMASTER L.L.C.
and LIVE NATION ENTERTAINMENT, INC.